United States Department of Defense
X.509 Certificate Policy

Version 10.1

19 February 2010

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

THIS PAGE INTENTIONALLY LEFT BLANK

1 INTRODUCTION

The United States Department of Defense (DoD) is developing a Key Management Infrastructure (KMI) to provide engineered solutions (consisting of products and services) for security of networked computer-based systems. Part of this KMI is a Public Key Infrastructure (PKI) consisting of products and services which provide and manage X.509 certificates for public key cryptography. Certificates identify the individual named in the certificate, and bind that person to a particular public/private key pair.

Programs which carry out or support the mission of the US DoD require services such as authentication, confidentiality, technical non-repudiation, and access control. These services are met with an array of network security components such as workstations, guards, firewalls, routers, in-line network encryptors (INE), and trusted database servers. The operation of these components is supported and complemented by use of public key cryptography. As a system solution, the components share the burden of the total system security. The use of public key certificates does not add any security services in a poorly designed or implemented system.

Security management services provided by the PKI include:

- Key Generation/Storage/Recovery;
- Certificate Generation, Update, Renewal, Re-key, and Distribution;
- Certificate Revocation List (CRL) Generation and Distribution;
- Directory Management of Certificate Related Items;
- Certificate token initialization/programming/management;
- Privilege and Authorization Management; and,
- System Management Functions (e.g., security audit, configuration management, archive).

The security of these services is ensured by defining requirements on PKI activities, including the following:

- Subscriber identification and authorization verification;
- Control of computer and cryptographic systems;
- Operation of computer and cryptographic systems;
- Usage of keys and public key certificates by Subscribers and relying parties; and,
- Definition of rules to limit liability and to provide a high degree of certainty that the stipulations of this policy are being met.

The reliability of the public key cryptography portion of the security solution is a direct result of the secure and trustworthy operation of an established PKI, including equipment, facilities, personnel, and procedures.

The applicability statements in this policy shall be considered minimum requirements; application accreditors may require higher levels of assurance than specified in this certificate policy for the stated applications.

1.1 OVERVIEW

The United States Department of Defense Certificate Policy (CP) is the unified policy under which a Certification Authority (CA) operated by a DoD component is established and operates. It does not define a particular implementation of PKI, nor the plans for future implementations or future Certificate Policies. It also does not define certificate policy for CAs operated by external entities on behalf of the DoD. This document will be reviewed and updated as described in Section 1.5, based on operational experience, changing threats, and further analysis.

This document defines the creation and management of Version 3 X.509 public key certificates for use in applications requiring communication between networked computer-based systems. Such applications include, but are not limited to, electronic mail; transmission of unclassified and classified information; signature of electronic forms; contract formation signatures; and authentication of infrastructure components such as web servers, firewalls, and directories. The network backbone for these network security products may be unprotected networks such as the Internet or Non-classified Internet Protocol Router Network (NIPRNET), or protected networks such as the Secret Internet Protocol Router Network (SIPRNET).

1.2 DOCUMENT NAME AND IDENTIFICATION

The DoD PKI has registered nine levels of assurance. Each level of assurance has been assigned an object identifier (OID) to be asserted in certificates issued by CAs who comply with the policy stipulations related to that level. The OIDs are registered under the id-infosec arc as:

{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) certificate-policy(11)}

id-US-dod-basic	ID::= {id-certificate-policy 2}
id-US-dod-medium	ID::= {id-certificate-policy 5}
id-US-dod-medium-2048	ID::= {id-certificate-policy 18}
id-US-dod-mediumHardware	ID::= {id-certificate-policy 9}
id-US-dod-mediumHardware-2048	ID::= {id-certificate-policy 19}
id-US-dod-PIV-Auth	ID::= {id-certificate-policy 10}
id-US-dod-PIV-Auth-2048	ID::= {id-certificate-policy 20}
id-US-dod-high	ID::= {id-certificate-policy 4}
id-US-dod-type1	ID::= {id-certificate-policy 6}

Except for the definitions provided in Section 1.4.1.6, this CP currently addresses only the policy stipulations required for a PKI to be approved to assert the DoD Medium {5}, Medium-2048 {18}, Medium Hardware {9}, Medium Hardware-2048 {19}, PIV-Auth {10}, PIV-Auth-2048 {20}, or High {4} Assurance OIDs.

The stipulations presented in this CP apply to all seven assurance levels (Medium, Medium-2048, Medium Hardware, Medium Hardware-2048, PIV-Auth, PIV-Auth-2048 and High) unless otherwise noted.

Unless otherwise stated, all references to “Medium Assurance” apply to Medium, Medium-2048, Medium Hardware, Medium Hardware-2048, PIV-Auth, and PIV-Auth-2048 certificates.

With the exception of key size, the requirements are identical for the following pairs of OIDs:

- Medium and Medium-2048;
- Medium Hardware and Medium Hardware-2048; and,
- PIV-Auth and PIV-Auth-2048.

Certificates asserting the PIV-Auth OID meet all of the requirements for Medium Assurance Hardware except that certificates that assert the PIV-Auth OID shall assert a key usage of digitalSignature and no other key usage. Certificates asserting the PIV-Auth-2048 OID meet all of the requirements for Medium Assurance Hardware-2048 except that certificates that assert the PIV-Auth-2048 OID shall assert a key usage of digitalSignature and no other key usage.

1.3 PKI PARTICIPANTS

The following sections introduce the PKI and community roles involved in issuing and maintaining key management certificates. These roles are described in detail in Section 5.2.

The DoD Policy Management Authority (PMA) is a body established by the Department to:

- oversee the creation and update of certificate policies, including evaluation of changes requested by DoD Services and Agencies, and plans for implementing any accepted changes; provide timely, responsive, DoD Service and Agency coordination to the DoD CP through a consensus-building process;
- review the Certification Practice Statements (CPSs) of DoD operated Certificate Management Authorities (CMAs) that offer to provide services to the DoD by analyzing the CPSs to ensure that the practices of CMAs serving the DoD comply with the DoD Certificate Policies;
- review the results of CMA compliance audits to determine if the CMAs are adequately meeting the stipulations of approved CPSs, and make recommendations to the CMAs regarding corrective actions, or other measures that might be appropriate, such as revocation of CMA certificates;

- establish the suitability of non-DoD policies for use within the DoD (for example, in cases where the technical mechanism of "policy mapping" is being considered); and,
- offer recommendations to the DoD Program and Project Managers and DoD Information System Accreditation Authorities regarding the appropriateness of certificates associated with the DoD certificate policies for specific applications.

PMA decision authority resides with the Office of the DoD Chief Information Officer, and its designees. The PMA may delegate authority in appropriate DoD policies and instructions.

Both Certification Authorities and Registration Authorities (RAs) are "Certificate Management Authorities" (CMAs). This policy will use the term CMA when a function may be assigned to either a CA or an RA, or when a requirement applies to both CAs and RAs. The term Registration Authority includes entities such as Local Registration Authorities. The division of Subscriber registration responsibilities between the CA and RA may vary among implementations of this certificate policy. This division of responsibilities shall be described in the CA's CPS.

Online Certificate Status Protocol (OCSP) Responders that comply with *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP* [RFC 2560] are also considered a CMA if issued a DoD PKI certificate.

1.3.1 Certification Authorities

A Certification Authority (CA) is an entity authorized by the PMA to create, sign, and issue public key certificates. A CA is responsible for all aspects of the issuance and management of a certificate, including control over the registration process, the identification and authentication process, the certificate manufacturing process, publication of certificates, revocation of certificates, and re-key; and for ensuring that all aspects of the CA services and CA operations and infrastructure related to certificates issued under this Policy are performed in accordance with the requirements, representations, and warranties of this Policy. CA is an inclusive term, and includes all types of CAs. Any CA requirement expressed in this Policy applies to all CA types unless expressly stated otherwise.

In the case of a hierarchical PKI, the CAs must be subordinate to a Root CA (and a maximum of one intermediate CA). The nature of the subordination shall be described in one or more Certification Practice Statements (CPSs) that have been generated for that hierarchy, and implemented through procedure and certificate extensions. The CA to which a second CA is subordinate is called the second CA's "superior CA."

1.3.2 Registration Authorities

A Registration Authority (RA) is an entity that enters into an agreement with a CA to collect and verify Subscribers' identity and information, which is to be entered into public key certificates. The RA must perform its functions in accordance with a CPS approved by the PMA.

1.3.3 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate, and who asserts that it uses its key and certificate in accordance with this policy. The targeted DoD PKI Subscribers include, but are not limited to, the following categories of entities that may wish to communicate securely and have demonstrated a bona fide need for a PKI certificate:

- DoD uniformed and civilian personnel, and eligible contractors;
- Executive department and agency personnel, and eligible contractors;
- State governments;
- Foreign government and foreign organization personnel, and eligible contractors; and,
- Workstations, guards and firewalls, routers, in-line network encryptors (INE), trusted servers (e.g., database, FTP, WWW), and other infrastructure components. These components must be under the cognizance of humans, who accept the certificate and are responsible for the correct protection and use of the associated private key.

CMAs are technically Subscribers to the PKI; however, the term Subscriber as used in this document refers only to non-CMA entities who request certificates.

1.3.4 Relying Parties

A Relying Party is the entity who, by using another's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate, relies on the validity of the binding of the Subscriber's name to a public key. A Relying Party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

1.3.5 Other Participants

The DoD relying parties shall have access to directory services to obtain PKI related information such as the certificates and CRLs.

CAs operating under this policy will require the services of other security, community, and application authorities, such as compliance auditors and attribute authorities. The CA shall identify, in its CPS, the parties responsible for providing such services, and the mechanisms used to support these services. More detail is given in Section 5.2.

1.4 CERTIFICATE USAGE

Certificates asserting a Policy OID defined in this document shall only be used for transactions related to DoD business. CAs must state this requirement in their CPSs and impose a requirement on Subscribers to abide by this limitation.

Security of the Defense Information Infrastructure (DII) is of great importance to the DoD. For the DoD to effectively carry out its mission, the information must be accurate, and available when needed, only to those authorized to receive it. Furthermore, the source of information claiming to be official must be identifiable and capable of authentication. The DoD is pursuing a layered security approach for the DII using a wide variety of security-enabled products including public key based technologies.

The DoD PKI must support the following security services: *confidentiality*, *integrity*, *authentication* and *technical non-repudiation.* The PKI supports these security services by providing Identification and Authentication (I&A), integrity, and technical non-repudiation through digital signatures, and confidentiality through key exchange. These basic security services support the long-term integrity of application data, but may not by themselves provide a sufficient integrity solution for all application circumstances. For example, when a requirement exists to verify the authenticity of a signature beyond the certificate validity period, such as contracting, other services such as trusted timestamp may be necessary. These solutions are application based, and must be addressed by Subscribers and Relying Parties. The PKI provides this support to a wide range of applications that protect various types of information as specified in Section 1.4.1.6:

- Administrative and Financial Information;
- National Security System Information (NSSI);
- Mission Assurance Category II (MAC II) Information;
- Mission Assurance Category I (MAC I) Information;
- Classified information up through Top Secret compartmented data; and,
- Electronic commerce

A single solution providing support to every application would appear to be desirable but because of different legal, security and national policy requirements for protection of the different categories of information, the most cost-effective solution is one which supports multiple assurance levels.

1.4.1 Appropriate Certificate Uses

1.4.1.1 Level of Assurance

The level of assurance associated with a public key certificate is an assertion by a CA of the degree of confidence that a Relying Party may reasonably place in the binding of a Subscriber's public key to the identity and privileges asserted in the certificate. Level of assurance depends on the proper registration of Subscribers and the proper generation and management of the certificate and associated private keys, in

accordance with the stipulations of this policy. Personnel, physical, procedural, and technical security controls contribute to the assurance level of the certificates issued by a certificate management system.

1.4.1.2 Factors in Determining Usage

The amount of reliance a Relying Party chooses to place on the certificate will be determined by various risk factors. Specifically, the value of the information, the threat environment, and the existing protection of the information environment are used to determine the appropriate level of assurance of certificates required to protect and authenticate the information.

1.4.1.3 Value of the Information

The value of the information has been separated into importance of the information relative to the achievement of DoD goals and objectives, particularly the warfighter's combat mission and electronic commerce applications. This includes the sensitivity of the information (e.g., classified or sensitive), criticality (e.g., mission categories as defined by *Information Assurance (IA)* [DoDD 8500.1]) or monetary value for electronic commerce applications.

Examples of data information values are:

Low Value Information:

- Mission Assurance Category III (MAC III) Data as defined in Section 1.6 of this CP.

Medium Value Information:

- Mission Assurance Category II (MAC II) data as defined in Section 1.6 of this CP.
- Data protecting small and medium value financial transactions (e.g., office supplies, books, travel claims, vehicles, payroll).

High Value Information:

- Mission Assurance Category I (MAC I) data as defined in Section 1.6 of this CP.
- High value financial transactions (e.g., aircraft and building purchases).

1.4.1.4 Threat

Threat is any circumstance or event with the potential to cause harm. In terms of information systems, harm includes destruction, disclosure, or modification of data, processes, or processing components. Threats to systems include environmental disasters, physical damage, system penetration, violation of authorization, human error, and communications monitoring or tampering. Three items to consider when assessing the threat posed by an adversary are its capability, risk tolerance, and access. DoD studies have concluded that a great majority of past compromises have involved insider threats.

1.4.1.5 Level of Environmental Protection

The DoD data networks on which the certificates described in this policy will be used will have various levels of protection. Examples of mechanisms that provide network protection include network encryption, physical isolation, High Assurance Guards (HAG), and firewall*s*. These mechanisms are used to create a collection of system high networks and enclaves. The probability of attack on protected networks is reduced because:

- access is limited to people authorized to use the network and its interconnection points with other networks (i.e., the guards or firewalls);
- even for those with access, risk tolerance must be high, due for example to the lack of anonymity on the network and its access points; and,
- the capabilities of an attacker inside the network are hampered by the lack of availability of hacker tools, and the difficulty of bringing them from the outside.

The true amount of risk reduction associated with using these mitigation mechanisms can only be determined by a system security evaluation.

Examples of differing levels of environmental protection are:

Highly Protected Environment:

- Networks that are protected either with encryption devices approved by the National Security Agency (NSA) for protection of classified data or via physical isolation, and that are certified for processing system-high classified data, where exposure of unencrypted data is limited to US citizens holding appropriate security clearances.

Moderately Protected Environment:

- Physically isolated unclassified, unencrypted networks in which access is restricted based on legitimate need.
- Networks protected by NSA approved Type 1 encryption, accessible by US-authorized foreign nationals.

Minimally Protected Environment:

- Unencrypted networks connected to the Internet or NIPRNET, either directly or via a firewall.

1.4.1.6 General Usage

This section contains definitions for nine levels of assurance and guidance for their application. The guidance is based on the previous discussion of information value and environmental protection. Emphasis is placed on two types of activity: Integrity and access control to information considered sensitive by the DoD, and information related to electronic financial transactions and other e-commerce. The final selection of the security mechanisms and level of strength and assurance requires a risk management process that addresses the specific mission and environment. The authority responsible for approving a specific level of assurance required for a particular implementation will vary from organization to organization, but will normally be the system accreditor acting in accordance with the applicability guidance that follows.

DoD Basic Assurance: This level is intended for applications handling unclassified information of low value in a Minimally or Moderately Protected Environment. DoD CAs will not issue BASIC certificates; the DoD shall issue Medium Assurance and High Assurance certificates exclusively. Access to DoD information resources shall never be allowed on the basis of Basic certificates. Basic certificates, (or non-DoD equivalent certificates) may be accepted by DoD relying parties for the purpose of authenticating or encrypting communication that does not access or process DoD information (e.g., meeting coordination, accessing web site information that has been cleared for unlimited distribution). These certificates may, for example, be issued by non-DoD commercial entities.

DoD Medium Assurance: This level is intended for applications handling unclassified medium value information in Moderately Protected Environments, unclassified high value information in Highly Protected Environments, and discretionary access control of classified information in Highly Protected Environments.

Guidance:

- All applications appropriate for Basic certificates;
- Digital signature services for Mission Assurance Category I (MAC I) and national security information on an encrypted network;
- Privacy and authentication in support of access control security services (e.g., separation of communities of interests) for access to classified Special Compartmented or Special Access information on networks protected using NSA approved Type 1 cryptography appropriate to the data being protected, or on networks that are physically isolated and approved to process the classified data; and,
- Acceptable non-repudiation for small and medium value financial transactions other than transactions involving issuance or acceptance of contracts and contract modifications. This would include acceptance and payment for small and medium value financial transactions, travel claims, payroll, etc.

DoD Medium-2048 Assurance: This level is intended for the same usage as DoD Medium Assurance but has larger key size as required by updated guidance from the National Institute of Standards and Technology.

DoD Medium Assurance Hardware: This level is intended for applications handling unclassified medium value information in Minimally Protected Environments, unclassified high value information in Moderately Protected Environments, and discretionary access control of classified information in Highly Protected Environments. This level is also intended for all applications operating in environments appropriate for Medium Assurance but which require a higher degree of assurance and technical non-repudiation.

This level is intended for applications performing contracting and contract modifications.

Guidance:

- All applications appropriate for Basic or Medium Assurance certificates.

DoD Medium Assurance Hardware-2048: This level is intended for the same usage as DoD Medium Assurance but has larger key size as required by updated guidance from the National Institute of Standards and Technology.

DoD PIV-Auth Assurance: This level is intended for any use appropriate for DoD Medium Assurance Hardware that does not require non-repudiation.

DoD PIV-Auth-2048 Assurance: This level is intended for the same usage as DoD PIV-Auth Assurance but has larger key size as required by updated guidance from the National Institute of Standards and Technology.

DoD High Assurance: This level is intended for applications handling high value unclassified information (Mission Assurance Category I (MAC I), NSSI) in Minimally Protected environments.

Guidance:

- All applications appropriate for Medium Assurance certificates;
- Digital signature services for unclassified Mission Assurance Category I (MAC I) or national security information in an unencrypted network;
- Protection (authentication and confidentiality) for information crossing classification boundaries when such a crossing is already permitted under a system security policy (e.g., sending unclassified information through a HAG from SIPRNET to NIPRNET); and,
- Technical non-repudiation for large value financial or electronic commerce applications.

DoD Type 1: This level is intended for applications handling classified material in Minimally Protected Environments, and authentication of material that would affect the security of classified systems.

General usage is summarized in the following table. The levels of assurance listed are minimums. Any application that requires information to cross a classification boundary requires High Assurance.

Value of Information	Protection of Network Environment		
	High	Moderate	Minimal
Low	Medium Assurance	Medium Assurance	Medium Assurance
Medium	Medium Assurance	Medium Assurance	Medium Assurance Hardware
High	Medium Assurance	Medium Assurance Hardware	High Assurance

1.4.2 Prohibited Certificate Uses

See Section 1.4.

1.5 POLICY ADMINISTRATION

1.5.1 Organization Administering the Document

The PMA is responsible for the definition, revision and promulgation of this policy. The PMA is the Office of the DoD Chief Information Officer, and its designees.

1.5.2 Contact Person

Questions regarding this CP should be directed to:

DOD PKI PROGRAM MANAGEMENT OFFICE
9800 SAVAGE RD STE 6584
FT GEORGE G MEADE MD 20755-6584

1.5.3 Person Determining CPS Suitability for the Policy

The PMA shall determine the suitability of any CPS to this policy.

1.5.4 CPS Approval Procedures

The organization owning a CPS shall submit the CPS to the PMA for compliance analysis with this CP at the given level of assurance. The PMA shall commission a compliance analysis study culminating in a written report that provides a summary of areas in which the CPS may not or does not comply with this CP. The PMA shall resolve these discrepancies prior to approving the CPS. The CMA must have a PMA approved CPS and meet all CP/CPS requirements prior to commencing operations. In some cases the nature of the system function, the type of communications, or the operating environment may require the additional approval of an authorized agency.

The Policy Management Authority is authorized to make the determination that other (non-DoD) CPs offer appropriately equivalent levels of assurance to the DoD CPs. The PKI may respond to such decisions by methods including but not limited to:

- issuing cross-certificates to other PKIs asserting other policies;
- including certificates issued by other PKIs and asserting other CPs, in DoD OCSP Responders; or,
- recommending CAs asserting other CPs for inclusion in DoD application trust lists.

DoD PMA shall make information regarding such equivalency determinations widely available to DoD relying parties.

1.5.5 Waivers

Normally, the PMA shall decide that variation in CMA practice is acceptable under a current policy, or the CMA shall request a permanent change to the policy. Policy waivers may be granted by the PMA to meet urgent, unforeseen operational requirements (such as those associated with ongoing military actions or a similar crisis). When a waiver is granted, the PMA shall post the waiver on a web site accessible by relying parties, and shall either initiate a permanent change to the policy, or shall place a specific time limit, not to exceed one year, on the waiver.

1.6 DEFINITIONS AND ACRONYMS

See Section 10.

2 PUBLICATIONS AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

Repositories that support a CA in posting information as required by this policy shall:

- maintain availability of the information as required by the certificate information posting and retrieval stipulations of this policy; and,
- provide access control mechanisms sufficient to protect repository information as described in Section 2.4.

The repository that is the primary source of CA certificates and/or CRLs for access by relying parties shall be available 24 hours a day, 7 days a week with a minimum overall availability of 99% per year including scheduled down time, which shall not exceed 0.5% per year. Repository availability calculations do not include network down-time.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

Each CA shall provide an on-line repository that is available to Subscribers and relying parties and that contains:

- issued encryption certificates that assert this Policy;
- a CRL;
- the CA's certificate for its certificate signing key; and,
- a copy of this Policy, including any waivers granted to the CA by the PMA.

Additionally, each CA shall provide an on-line repository that is available to Subscribers with certificates asserting this Policy that includes sections of the CPS that describes Subscriber duties and responsibilities.

2.3 TIME OR FREQUENCY OF PUBLICATION

Certificates are published following Subscriber acceptance as specified in Section 4.4 and proof of possession of private key as specified in Section 3.2.1. The CRL is published as specified in Section 4.9.7. All information to be published in the repository shall be published promptly after such information becomes available to the CA. The CA shall specify in its CPS time limits within which it will publish various types of information.

2.4 ACCESS CONTROLS ON REPOSITORIES

Repository information shall be protected from unauthorized modification and disclosure.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

All certificates shall use DN name forms for the issuer and subject name fields.

In general, CAs shall not assign DNs. Subscribers shall have DNs assigned to them through their organizations, in accordance with a naming authority (see Section 3.1.2). The CMA shall investigate and correct if necessary any name collisions brought to its attention. If appropriate, the CMA shall coordinate with and defer to the appropriate naming authority. Some certificates may additionally assert an alternate name form. Details related to this requirement are provided in Section 7.1.4.

Medium Assurance, High Assurance	Non-null Subject Name, and optional Subject Alternative Name if marked non-critical

3.1.2 Need of Names to be Meaningful

Names used within the DoD shall identify the person or object to which they are assigned. The CMA shall ensure that an affiliation exists between the Subscriber and any organization that is identified by any component of any name in its certificate.

When DNs are used, the common name shall represent the Subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name. For equipment, this may be a model name and serial number, or an application process (e.g., Organization X Mail List, Organization Y Multifunction Interpreter).

The DoD will establish one or more authorities for the creation of DNs. A CMA who uses DNs will coordinate with such an authority to determine the proper elements for a given Subscriber.

Each root CA asserting this policy shall only sign certificates with subject names from within a name-space approved by the PMA. In the case where one CA certifies another, the certifying CA must impose restrictions on the name space authorized in the subordinate CA, which are at least as restrictive as its own name constraints.

When technical means exist for imposing these constraints (such as the name constraints certificate extension), they shall be used. Otherwise, these constraints shall be imposed procedurally or contractually.

3.1.3 Anonymity or Pseudonymity of Subscribers

A CA shall not issue anonymous certificates. CA certificates shall not contain anonymous or pseudonymous identities.

3.1.4 Rules for Interpreting Various Name Forms

Rules for interpreting name forms are contained in the applicable certificate profile (see Section 7.1.2), and are established by a naming authority if one exists, or by the CA itself. The naming authority shall be identified contractually or in a CPS.

3.1.5 Uniqueness of Names

Name uniqueness across the DoD must be enforced. Wherever practical, X.500 DNs allocated from a DoD naming authority shall be used, and the CAs and RAs shall enforce name uniqueness within the X.500 name space, which they have been authorized. When other name forms are used, they too must be allocated such that name uniqueness across the DoD is ensured. A CA shall document in its CPS what name forms will be used, how the CA and RAs will interact with DoD naming authorities, and how they will allocate names within the Subscriber community to guarantee name uniqueness among current and past Subscribers (i.e., if “Joe Smith” leaves a CA’s community of Subscribers, and a new, different “Joe Smith” enters the community of Subscribers, how will these two people be provided unique names).

3.1.6 Recognition, Authentication and Role of Trademarks

A CMA is not required to issue a name that contains a requested trademark. A CMA shall not issue a certificate knowing that it includes a name that a court of competent jurisdiction has determined infringes the trademark of another. A CMA is not required to issue subsequently a name containing a requested trademark if the CMA has already issued one sufficient for identification within the DoD. A CMA is not obligated to research trademarks or resolve trademark disputes.

3.2 INITIAL IDENTITY VALIDATION

The requirements of Section 3.2 apply to all Subscribers including Trusted Roles.

3.2.1 Method to Prove Possession of Private Key

In all cases where the Subscriber generates keys, the Subscriber shall be required to prove, to the CMA, possession of the private key, which corresponds to the public key in the certificate request. For signature keys, this may be done by signing the request. For key management keys, the CA or RA may encrypt the Subscriber's certificate in a confirmation request message. The Subscriber can then decrypt and return the certificate to the CA or RA in a confirmation message. The PMA may determine other mechanisms that are at least as secure as those cited here to be acceptable.

In the case where key is generated directly on the Subscriber's token, or in a key generator that benignly transfers the key to the Subscriber's token, then the Subscriber is in possession of the private key at the time of generation or transfer. If the Subscriber is not in possession of the token when the key is generated, then the token shall be delivered to the Subscriber via an accountable method (see Section 6.1.2).

3.2.2 Authentication of Organization Identity

Requests for certificates in the name of an organization shall include the organization name, address, and documentation of the existence of the organization. The CMA shall verify this information, in addition to the authenticity of the requesting representative, and that representative's authorization to act in the name of the organization. Use of organization certificates shall be addressed in the appropriate CMA CPS and these CMAs shall preclude the use of organization certificates where individual non-repudiation is required.

Public key certificates shall be issued in the name of an individual whenever possible, and the private keys associated with such certificates shall never be shared with any other person. For those cases where there must be several persons acting in one role or in a group, a certificate may be issued with a Distinguished Name that identifies the group or role. Alternatives for issuing group or role certificates are listed below in order of preference. Less secure options shall only be used if more highly preferred options are not feasible.

- Unique signature and encryption keys and associated certificates containing the group or role name shall be issued to components acting on behalf of or mediating for a group or role (e.g., mail list agents).
- Each individual acting in the same role shall have a separate private signature key and a certificate indicating the role. The individuals acting in the same role or group may share the same encryption certificate and associated private key.
- A signature certificate containing a distinguished name that indicates the role may be issued, and the associated signature private key may be shared by persons acting in that role. (Note that the lack of technically-enforced individual accountability and reliance on procedural mechanisms as described in the requirements below represents a greater security risk to the systems and data protected using these certificates, and must thus be limited to the maximum extent possible. As non-repudiation can no longer be proven, certificates corresponding to private keys held by multiple Subscribers shall not be used for contracting or e-commerce applications.)

A local authority shall authorize the creation of group or role certificates. In these cases:

- The group/role Sponsor shall be responsible for ensuring control of the private key and tracking who possesses the private key at all times, including maintaining an ongoing list of Subscribers who have access to use of the private key and also listing, which Subscriber had control of the

key at what time. The group/role Sponsor shall forward an initial list and periodically forward all updates since the last submission of this list to the local Information System Security Officer (ISSO).

- The ISSO is responsible for periodically reviewing the Sponsor's list with an eye towards identification of anomalies.
- A list of those holding the shared private key will be made available to the CA and RA, upon request.

The procedures for issuing tokens for use in shared key applications must comply with all other stipulations of this Policy (e.g., key generation, private key protection, Subscriber obligations).

3.2.3 Authentication of Individual Identity

3.2.3.1 In-Person Authentication

The CMA shall ensure that the applicant's identity information and public key are bound adequately. Each CMA shall specify in its CPS procedures for authenticating a Subscriber's identity. Additionally a CMA shall record the process that was followed for each certificate. At a minimum, process documentation must include:

- the identity of the person performing the identification;
- a signed declaration by the person that verified the identity of the Subscriber as required by this certificate policy;
- the method used to authenticate the individual's identity, including identification type and unique numeric or alphanumeric identifier if appropriate; and,
- the date of the verification.

Additionally, the process documentation must include a declaration of identity. The declaration shall be signed with a handwritten signature or, if a good fingerprint or other adequate biometric is collected and can be linked to the Subscriber identity, a digital signature. Either signature must be applied in the presence of the person performing the identity authentication.

For Medium Assurance and High Assurance applicant identity proofing requires the applicants to provide at least one federal government official picture identification credential (such as a DoD identification card or passport), or two non-federal government issued official identification credentials, at least one of which must be a photo ID, such as a drivers license. As an alternative to presentation of identification credentials, other mechanisms of equivalent or greater assurance (such as comparison of biometric data to identities pre-verified to the standards of this policy, and obtained via authenticated interaction with secured databases) may be used.

For Medium Assurance, the applicant's identity must be personally verified prior to the applicant's certificate being enabled. The applicant shall appear personally before either:

- A CMA;
- A Trusted Agent (TA) personally approved by the CMA or appointed by name in writing to the CMA by the Commanding Officer/Officer in Charge of the organization which they represent; or,
- A person certified by the US Federal Government or a state government as being authorized to confirm identities such as Notaries Public, that uses a stamp, seal or other mechanism to authenticate their identity confirmation. In addition, the CPS shall specify how notification will be provided that this identity proofing has occurred and how it will be verified that the appropriate official performed the identity proofing.

The applicant shall appear before one of the required identity verifiers no more than 30 days prior to application of the CA's signature to the applicant's certificate, or alternatively, when private keys are delivered to Subscribers via hardware tokens, the Subscribers shall personally appear before the CMA or CMA's TA to obtain their tokens or token activation data.

For Medium Assurance Hardware or High Assurance, a CMA shall personally verify the applicant's identity prior to the applicant's certificate being enabled. There are two ways to meet this requirement:

- The applicant shall personally appear before the CMA, or a TA personally approved by the CMA or appointed by name in writing to the CMA by the Commanding Officer/Officer in Charge of the organization which they represent, at any time prior to application of the CA's signature to the applicant's certificate; or,
- When private keys are delivered to Subscribers via hardware tokens, the Subscribers shall personally appear before the CMA to obtain their tokens or token activation data. However, Key Transfer Cards which contain only an encryption private key for use in FORTEZZA/CAW remote re-key may be delivered to the Subscriber by a TA to facilitate the issuance of operational Subscriber certificates in accordance with the requirements of this policy.

Minors and others not competent to perform face-to-face registration alone shall be accompanied by a person already certified by the PKI, who will present information sufficient for registration at the level of the certificate being requested, for both himself and the person accompanied.

Medium Assurance	Must appear in person to a TA, Notary (or equivalent), or CMA, and present official picture ID
Medium Assurance Hardware or High Assurance	Must appear in person to CMA or TA, and present official picture ID

3.2.3.2 Electronic Authentication

Medium Assurance, Medium Assurance Hardware or High Assurance certificates may be issued on the basis of electronically authenticated (using a current, valid DoD PKI signature certificate and associated private key) Subscriber requests, subject to the following restrictions:

- The assurance level of the new certificate shall be the same or lower than the assurance level of the existing certificate used as an authentication credential;
- The DN of the new certificate shall be identical to the DN of the signature certificate. Information in the new certificate that could be used for authorization shall be identical to that of the signature certificate;
- The expiration date of the new certificate will be no later than the next required in-person authentication date associated with the signature certificate;
- The in-person authentication date associated with a new certificate will be no later than the in-person authentication date associated with the signature certificate used for authentication; and,
- The validity period of the new certificate shall not be greater than the maximum validity period requirements of this CP for that type of certificate.

Electronically authenticated issuance is similar to certificate re-key (Section 3.3) except that the new certificate is valid concurrently with the existing certificate, but with a potentially different expiration date.

3.2.3.3 Authentication of Component Identities

Some computing and communications components (e.g., routers, firewalls) will be named as certificate subjects. In such cases, the component must have a human PKI Sponsor as described in Section 5.2.1.4. The PKI Sponsor is responsible for providing the CMA, or to CMA approved TAs as described in Sections 3.2.3.1 and 5.2.1.4, correct information regarding:

- equipment identification;
- equipment public keys;
- equipment authorizations and attributes (if any are to be included in the certificate); and,
- contact information to enable the CMA to communicate with the PKI sponsor when required.

The CMA, or their TAs, shall authenticate the validity of any authorizations to be asserted in the certificate, and shall verify source and integrity of the data collected to an assurance level commensurate with the

certificate being requested. Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from PKI sponsors (using certificates of equivalent or greater assurance than that being requested).
- In person registration by the PKI Sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 3.2.3.1.

3.2.4 Non-Verified Subscriber Information

Subscriber e-mail address included in the certificate (e.g., in the subject alternative name extension) is not verified.

3.2.5 Validation of Authority

Certificates that contain explicit or implicit organization affiliations shall be issued only after ascertaining the Subscriber has the authorizations to act on behalf of the organization in the implied capacity. Examples of these include group and role certificates, and CA and RA certificates.

3.2.6 Criteria for Interoperation

The US Federal Public Key Infrastructure (FPKI) Certificate and CRL Profile, FPKI Directory Interoperability Profile, and DoD X.509 CP shall form a basis for assessing interoperability with the DoD PKI. However, the decision to cross certify with an external PKI shall reside with the PMA as specified in Section 1 of this CP.

3.3 Identification and Authentication for Re-Key Requests

The longer and more often a key is used, the more susceptible it is to loss or discovery. This weakens the assurance provided to a Relying Party that the unique binding between a key and its named Subscriber is valid. Therefore, it is important that a Subscriber periodically obtains new keys and re-establishes its identity. Re-keying a certificate means that a new certificate is created that is identical to the old one, except that the new certificate has a new, different public key (corresponding to a new, different private key); a different serial number; and may be assigned a different validity period.

Subscriber certificates may be rekeyed on the basis of existing Subscriber certificates as long as:

- The validity period of the new certificate would not exceed the maximum time period between face-to-face authentications as required by Section 3.3.1;
- The maximum life of the new certificate shall not exceed 3 years;
- The assurance level of the new certificate is the same or less than the certificate used to authenticate the request; and,
- All other Subscriber information remains valid.

If the above is not true, the Subscriber must meet the initial identity validation requirements listed in Section 3.2.

Any CA who includes authorizations in a certificate, including any conveyed or implied by the subject's DN, shall document in its CPS the mechanisms used to notify the CA of the withdrawal of authorization. Withdrawal of authorization shall result in revocation of the old certificate and, if necessary, the issuance of a new certificate with a different public key and the appropriate authorizations.

Subscribers signature private keys and certificates have a maximum lifetime of three years. Subscriber key management certificates have a maximum lifetime of three years; use of Subscriber key management private keys for decryption is unrestricted.

CA key lifetimes are provided in Section 5.6.

3.3.1 Identification and Authentication for Routine Re-Key

Re-key requests for certificates can be authenticated on the basis of current valid Subscriber certificates as long as the validity period of the new certificate does not extend beyond the periodic in-person authentication requirements listed in the table below.

Assurance Level	In-Person Authentication Requirement
Medium Assurance Software	Every 9 years
Medium Assurance Hardware	Every 4 years
High Assurance	Every 3 years

CA identity shall be validated through use of the current signature key or initial registration process. Identity shall be established through initial registration process at least once every three years.

3.3.2 Identification and Authentication for Re-Key After Revocation

Re-key after revocation for all assurance levels shall be done using in-person authentication in accordance with Section 3.2.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests must be authenticated; see Section 4.9.3. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

It is the intent of this Policy to identify the minimum requirements and procedures that are necessary to support trust in the PKI, and to minimize imposition of specific implementation requirements on CMAs, Subscribers, and relying parties.

The applicant and the CMA must perform the following steps when an applicant applies for a certificate:

- establish and record identity of Subscriber (per Section 3.2);
- obtain a public/private key pair for each certificate required;
- establish that the public key forms a functioning key pair with the private key held by the Subscriber (per Section 3.2.1); and,
- provide a point of contact for verification of any roles or authorizations requested.

These steps may be performed in any order that is convenient for the CMA and Subscribers, and that does not defeat security; but all must be completed prior to certificate issuance. All communications among CMAs supporting the certificate application and issuance process shall be authenticated and protected from modification using mechanisms commensurate with the requirements of the data to be protected by the certificates being issued (i.e., communications supporting the issuance of Medium Assurance certificates shall be protected using Medium Assurance certificates, or some other mechanism of equivalent strength). Any electronic transmission of shared secrets shall be protected (e.g., encrypted) using means commensurate with the requirements of the data to be protected by the certificates being issued.

CAs implementing this CP shall certify other CAs (to include cross-certification) only as authorized by the DoD PMA.

Requests by CAs for CA certificates shall be submitted to the DoD PMA using the contact provided in Section 1.5, and shall be accompanied by a CPS written to the format of the *Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework* [RFC 3647].

The DoD PMA will evaluate the submitted CPS for acceptability. The PMA may require an initial compliance audit, performed by parties of the PMA's choosing, to ensure that the CMA is prepared to implement all aspects of the submitted CPS, prior to the DoD PMA authorizing the CMA to issue and manage certificates asserting the DoD CPs.

CAs shall only issue certificates asserting DoD CPs upon receipt of written authorization from the DoD PMA, and then may only do so within the constraints imposed by the PMA or its designated representatives.

4.1.1 Who Can Submit a Certificate Application

Certificate application may be submitted to the CA by the Subscriber, or an RA/LRA on behalf of the Subscriber.

4.1.2 Enrollment Process and Responsibilities

Upon receiving the request, the CMA or TA will:

- verify the identity of the requestor; and,
- verify the authority of the requestor and the integrity of the information in the certificate request.

While the Subscriber may do most of the data entry, it is still the responsibility of the CMA to verify that the information is correct and accurate. This may be accomplished either through a system approach linking databases containing personnel information or through personal contact with the program's attribute authority (as put forth in the CMA's CPS). If databases or other sources are used to confirm Subscriber attributes, then these sources and associated information sent to a CMA must be protected from unauthorized modification to a level commensurate with the level of assurance specified for the certificates conveying the Subscriber attributes. CMAs shall verify all authorization and other attribute information

received from an applicant. In most cases, the RA is responsible for verifying applicant data, but if CAs accept applicant data directly from applicants, then the CA is responsible for verifying the applicant data. Information regarding attributes shall be verified via those offices or roles that have authority to assign the information or attribute. Relationships with these offices or roles shall be established prior to commencement of CA duties, and shall be described in a CPS.

4.2 CERTIFICATE APPLICATION PROCESS

It is the responsibility of the CA and RA to verify that the information in certificate applications is accurate. Their CPSs shall specify procedures to verify information in certificate applications.

4.2.1 Performing Identification and Authentication Functions

The identification and authentication of the Subscriber shall be done by the CA, RA, LRA, or a TA on behalf of these parties.

4.2.2 Approval or Rejection of Certificate Applications

The certificate application may be rejected for various reasons such as inaccurate information or lack of mission need to provide a certificate to the Subscriber. The CA, RA, LRA, or TA may reject a certificate application. The CA, RA, LRA, or TA shall work with the appropriate parties to resolve the problem.

A certificate application shall not be considered accepted until the CA has accepted the application and decided to issue a certificate.

4.2.3 Time to Process Certificate Applications

No stipulation.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions During Certificate Issuance

The CA shall authenticate a certificate request, ensure that the public key is bound to the correct Subscriber, obtain a proof of possession of the private key, then generate a certificate, and provide the certificate to the Subscriber. The CA shall publish the certificate to a repository in accordance with Section 4.4.2.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

The Subscriber shall be notified of certificate issuance.

4.4 CERTIFICATE ACCEPTANCE

4.4.1 Conduct Constituting Certificate Acceptance

For in-person authentication, the Subscriber signature on a certificate acceptance and acknowledgment of responsibilities form (e.g., DD Form 2842) shall constitute acceptance of the certificate. The Subscriber signature shall be collected before a CA allows a Subscriber to make effective use of its private key.

For electronic authentication, the Subscriber request to obtain new certificates and subsequent failure to object to the certificate or its contents shall constitute acceptance of the certificate.

4.4.2 Publication of the Certificate by the CA

CA certificates and Subscriber encryption certificates shall be published to the appropriate repositories.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

The Subscriber shall not use the signature private key after the associated certificate has been revoked or has expired.

The Subscriber may continue to use the decryption private key solely to decrypt previously encrypted information after the associated certificate has been revoked or has expired.

The Subscriber shall use the private key for DoD business only. The use of the private key shall be further limited in accordance with the key usage extension in the certificate.

If the extended key usage extension is present and implies any limitation on the use of the private key, those constraints shall also be observed. For example, the OCSP Responder private key shall be used only for signing OCSP responses.

4.5.2 Relying Party Public Key and Certificate Usage

The relying parties shall ensure that a public key in a certificate is used only for the purposes indicated by the key usage extension, if the extension is present.

If the extended key usage extension is present and implies any limitation on the use of the certificate, those constraints shall also be followed.

4.6 CERTIFICATE RENEWAL

Renewing a certificate means creating a new certificate with the same name, key, and authorizations as the old one, but with an extended validity period and new serial number. Certificates may be renewed as a means of CRL size management. A certificate may be renewed if the public key has not reached the end of its validity, the associated private key has not been compromised, and the Subscriber name and attributes are correct. Thus, a CMA may choose to implement a three-year re-key period with an initial issue and two annual renewals. The old certificate need not be revoked, but must not be further re-keyed, renewed, or updated.

4.6.1 Circumstance for Certificate Renewal

A certificate may be renewed if the certificate has not reached the end of its validity period, the certificate has not been revoked, the total life times of certificates issued (including the new certificate) for that public key do not exceed the times listed below, and the Subscriber name and attributes are still correct.

Assurance Level	Time
Medium Assurance Software	3 Years
Medium Assurance Hardware	3 Years
High Assurance	3 Years

4.6.2 Who May Request Renewal

The Subscriber, RA, or LRA may request the renewal of a Subscriber certificate.

4.6.3 Processing Certificate Renewal Requests

- The renewal process could be akin to the initial certificate issuance process described in Sections 3.2.3.1 and 4.3.
- Alternatively, the certificate could be automatically renewed by the CA based on an electronically authenticated request from the Subscriber as per Section 3.2.3.2.

4.6.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

See Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to other Entities

See Section 4.4.3.

4.7 CERTIFICATE RE-KEY

Re-keying a certificate means creating a new certificate with the same name and authorizations as the old one, but with a new key, extended validity period and new serial number. After certificate rekey, the old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

4.7.1 Circumstance for Certificate Re-Key

A certificate shall be re-keyed when it can no longer be renewed as described in Section 4.6.1.

A revoked certificate shall not be re-keyed.

Requirements for CA re-key are described in Section 5.6.

4.7.2 Who May Request Certification of a New Public Key

The Subscriber, RA, or LRA may request the re-key of a Subscriber certificate.

4.7.3 Processing Certificate Re-Keying Requests

The re-key process could be akin to the initial certificate issuance process described in Section 4.3. Alternatively, the certificate could be automatically re-keyed by the CA based on an electronically authenticated request from the Subscriber as per Section 3.2.3.2.

4.7.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

See Section 4.4.1.

4.7.6 Publication of the Re-Keyed Certificate by the CA

See Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.8 CERTIFICATE MODIFICATION

Modifying (updating) a certificate means creating a new certificate that has the same or a different key, a different serial number, and differs in one or more other fields, from the old certificate. For example, a CA may choose to modify a certificate of a Subscriber who gains an authorization. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or modified.

The CA shall authenticate the validity of any authorizations using the same means as for the initial authorization or means of equal or greater security and assurance.

4.8.1 Circumstance for Certificate Modification

A certificate may be modified if some of the information other than the DN, such as the e-mail address or authorizations, has changed.

If the Subscriber name has changed, the Subscriber shall undergo the initial registration process.

4.8.2 Who May Request Certificate Modification

The Subscriber, RA, or LRA may request the modification of a Subscriber certificate. Any change in authorizations must be validated by the CA, RA, or the LRA.

4.8.3 Processing Certificate Modification Requests

The certificate modification process could be akin to the initial certificate issuance process described in Section 4.3. Alternatively, the certificate could be automatically modified by the CA based on an electronically authenticated request from the Subscriber as per Section 3.2.3.2. However, any change in authorizations must be validated by the CA, RA, or the LRA.

4.8.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

See Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

See Section 4.4.2.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

A certificate shall be revoked when the binding between the subject and the subject's public key defined within a certificate is no longer considered valid. Examples of circumstances that invalidate the binding are:

- identifying information or affiliation components of any names in the certificate become invalid;
- privilege attributes asserted in the Subscriber's certificate are reduced;
- the Subscriber can be shown to have violated the stipulations of its Subscriber agreement;
- the private key is suspected of compromise; and,
- the Subscriber or other authorized party (as defined in the CMA's CPS) asks for his/her certificate to be revoked.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the CRL. In addition, if it is determined subsequent to issuance of new certificates that a private key used to sign requests for one or more additional certificates may have been compromised at the time the requests for additional certificates were made, all certificates authorized by directly or indirectly chaining back to that compromised key shall be revoked. Revoked certificates shall be included on all new publications of the CRL until the certificates expire.

4.9.2 Who Can Request a Revocation

Within the PKI, a CMA may summarily revoke certificates within its domain. A written notice and brief explanation for the revocation shall subsequently be provided to the Subscriber. The RA can request the revocation of a Subscriber's certificate on behalf of any authorized party as specified in its CPS.

4.9.3 Procedure for Revocation Request

Any format that is used to request a revocation shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed). A CMA action is required for revocation (a Subscriber may not, via an automated process, revoke its own certificate or change a prior revocation reason without CMA intervention). Authentication of certificate revocation requests is important to prevent malicious revocation of certificates by unauthorized parties.

In particular, if the revocation is being requested for reason of key compromise or suspected fraudulent use, then the Subscriber's and the RA's revocation request must so indicate. If an RA performs this on behalf of a Subscriber, a formal, signed message format known to the CA shall be employed. All requests shall be authenticated; for signed requests from the certificate subject, or from an RA, verification of the signature is sufficient.

Upon receipt of a revocation request from the Subscriber or another authorized party, the CMA shall authenticate the revocation request. The CMA may, at its discretion, take reasonable measures to verify the need for revocation. If the revocation request appears to be valid, the CMA shall revoke the certificate by placing its serial number and other identifying information on a CRL, in addition to any other revocation mechanisms used.

For PKI implementations using hardware tokens, Subscribers leaving organizations that sponsored their participation in the PKI shall surrender to their CMA (through any accountable mechanism) all cryptographic hardware tokens that were issued under the sponsoring organization prior to leaving the organization. The token shall be zeroized or destroyed promptly upon surrender and shall be protected from malicious use between surrender and zeroization or destruction.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation under this policy; Subscribers and authorized PKI entities shall request the revocation of a certificate as soon as the need for revocation comes to their attention.

4.9.5 Time Within Which CA Must Process the Revocation Request

The CA shall process all revocation requests within one hour of receipt. CRL issuance frequency is addressed in Section 4.9.7.

4.9.6 Revocation Checking Requirements for Relying Parties

Use of revoked certificates could have damaging or catastrophic consequences in certain applications. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party and the system accreditor. If it is temporarily infeasible to obtain revocation information, then the Relying Party must either reject use of the certificate, or make an informed decision to accept the risk, responsibility, and consequences for using a certificate whose authenticity cannot be guaranteed to the standards of this policy. Such use may occasionally be necessary to meet urgent operational requirements.

4.9.7 CRL Issuance Frequency

CRLs are periodically issued and posted to a repository, even if there are no changes or updates to be made, to ensure timeliness of information. CRLs may be issued more frequently than required; if there are circumstances under which a CA will post early updates, these shall be spelled out in its CPS. CAs shall ensure that superseded CRLs are removed from the repository upon posting of the latest CRL.

The DoD CAs shall conform to the CRL issuance frequency described below:

CA	Normal CRL Issuance Periodicity	Maximum CRL Issuance Latency for the Reason of Key or CA Compromise
Medium Assurance, Medium Hardware Assurance Root CA	At least once every 28 days	Within 18 hours of notification
Medium Assurance, Medium Hardware Assurance Signing CA	At least once each day	Within 18 hours of notification
High Assurance Root CA	At least once every 28 days	Within 6 hours of notification
High Assurance Signing CA	At least once each day	Within 6 hours of notification
FORTEZZA PAA, PCA, CAW	At least once every 28 days	Within 6 hours of notification

High Assurance Subscriber certificates, when revoked for reason of key compromise, shall be listed on an Indirect Certificate Revocation List (ICRL), in accordance with [SDN 706], or some mechanism of equivalent functionality and timeliness, within six hours of receipt of the revocation request by an infrastructure component (RA or CA). A High Assurance CA certificate, revoked for any reason, shall also be placed on the High Assurance ICRL in accordance with [SDN 706], or some mechanism of equivalent functionality and timeliness, within six hours of receipt of the revocation request.

CAs shall make public a description of how to obtain revocation information for the certificates they publish, and an explanation of the consequences of using dated revocation information. This information shall be given to Subscribers during certificate request or issuance, and shall be readily available to any potential Relying Party.

In the case of any DoD PKI CA revocation the DoD Root CA shall notify all cross certified or DoD approved external PKIs within the constraints of the table above.

4.9.8 Maximum Latency for CRLs

The CRL shall be posted upon generation, but within no more than four hours after generation. Furthermore, a new CRL shall be published no later than the time specified in the nextUpdate field of the most recently published CRL for the same CRL Scope.

4.9.9 On-Line Revocation/Status Checking Availability

CAs and Relying Party client software may optionally support on-line status checking. Since the DoD operates in some environments that cannot accommodate on-line communications, all CAs shall be required to support CRLs. Client software using on-line revocation checking need not obtain or process CRLs.

OCSP Responders shall function in a manner that ensures that:

- Accurate and up-to-date information from the authorized CA is used to provide the revocation status; and,
- Revocation status responses provide authentication and integrity services commensurate with the assurance level of the certificate being checked.

4.9.10 On-Line Revocation Checking Requirements

Relying Parties may optionally use on-line status checking. Since the DoD operates in some environments that cannot accommodate on-line communications, all CAs shall be required to support CRLs. Client software using on-line revocation checking need not obtain or process CRLs.

DoD relying parties (including CMAs) shall only rely upon OCSP Responders approved in accordance with the requirements of Section 9.6.5.

4.9.11 Other Forms of Revocation Advertisements Available

A CA may also use other methods to publicize the certificates it has revoked. Any alternative method must meet the following requirements:

- The alternative method must be described in the CA's approved CPS;
- The alternative method must provide authentication and integrity services commensurate with the assurance level of the certificate being verified; and,
- The alternative method must meet the issuance and latency requirements for CRLs stated in Sections 4.9.7 and 4.9.8.

4.9.12 Special Requirements Related to Key Compromise

A CMA using reason codes must have the ability to transition any reason code to compromise. Stipulations for CRL issuance due to key compromise are provided in Section 5.7.3.

4.9.13 Circumstances for Suspension and Restoration

CAs may support certificate suspension and restoration.

Certificate suspension occurs by marking the certificate as revoked with a reason code of "On Hold." These certificates shall be placed on the next CRL and shall remain on the CRL until the certificate is restored or the certificate expires.

A certificate is restored when the RA reinstates it.

Certificates that are marked as revoked with a reason code other than "On Hold" shall not be restored. The CA shall provide technical mechanisms to enforce this requirement.

4.9.13.1 Circumstances for Suspension

For CAs that support suspension, a certificate shall be suspended when there is reason to believe that the binding between the subject and the subject's public key defined within a certificate is not currently valid, or there may be reason to question the security of the private key, but additional research is necessary to fully determine the status. An example of a circumstances that may lead to certificate suspension are is a Subscriber is known or believed to have the token containing the private key associated with the certificate, and fails to appear at an expected duty location.

Suspension requests may be made for other purposes.

4.9.13.2 Circumstances for Restoration

For CAs that support restoration, a suspended certificate may be restored when the binding between the subject and the subject's public key defined within a certificate is determined to still be valid or the question of the security of the private key is resolved and there was no compromise of the private key. An example of a circumstance that may result in certificate restoration is, a Subscriber returns to duty in possession of the token and verifies it was always under appropriate control.

4.9.14 Who Can Request Suspension and Restoration

4.9.14.1 Who Can Request Suspension

Any member of the Subscriber's or PKI Sponsor's chain of command is authorized to request suspension of certificates.

4.9.14.2 Who Can Request Restoration

Any member of the Subscriber's or PKI Sponsor's chain of command is authorized to request restoration of certificates.

4.9.15 Procedure for Suspension and Restoration Requests

4.9.15.1 Procedure for Suspension Request

Any format that is used to request a suspension shall identify the certificate to be suspended, explain the reason for suspension, include an estimated time for the resolution of the suspension, and allow the request to be authenticated (e.g., digitally or manually signed). Digital authentication shall use a certificate at the same or higher assurance level as the certificate to be suspended.

Prior to approving a certificate suspension, the RA shall verify the suspension request, to include authenticating the identity of the requestor and verifying the requestor's authority to request revocation and the validity of the reason for the suspension request.

Once approved by the RA, the CA shall mark the certificate as suspended on the issuing CA which shall place its serial number and other identifying information on a CRL.

If the RA suspends a certificate because there is reason to suspect compromise of the private key, the maximum latency for CRL issuance shall be the latency specified for Reason of Key or CA Compromise in Section 4.9.7.

4.9.15.2 Procedure for Restoration Request

Any format that is used to request a restoration shall identify the certificate to be restored, explain the reason for restoration, and allow the request to be authenticated (e.g., digitally or manually signed) at a level commensurate with the certificate being restored. The RA shall validate all restoration requests to ensure that they have appropriate justification and were requested by an authorized entity to prevent malicious restoration of compromised certificates by unauthorized parties.

The private key associated with any suspended certificate shall not be used to authenticate the identity of the restoration requestor.

4.9.16 Limits on Suspension Period

Suspended certificates shall be periodically reviewed to determine if the reason for suspension remains valid. The RA that approved a suspension request shall review suspended certificates monthly or at the time specified in the suspension request, whichever is shorter. The RA shall then revoke any certificate where the suspension has exceeded the original requested suspension period and for which the requestor has not submitted an extension request following the same procedures as the initial request.

4.10 CERTIFICATE STATUS SERVICES

The DoD PKI does not support Certificate Status Authorities such as Simple Certificate Validation Protocol (SCVP).

4.10.1 Operational Characteristics

Not applicable. The DoD PKI does not use Certificate Status Authorities such as SCVP.

4.10.2 Service Availability

Not applicable. The DoD PKI does not use Certificate Status Authorities such as SCVP.

4.10.3 Optional Features

Not applicable. The DoD PKI does not use Certificate Status Authorities such as SCVP.

4.11 END OF SUBSCRIPTION

Subscription is synonymous with the certificate validity period. The subscription ends when the certificate is revoked or expired.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy and Practices

The DoD key escrow recovery policy is described in Key Recovery Policy (KRP) for the United States Department of Defense [KRP]. As required by [KRP], key escrow and recovery operations shall conform to an approved Key Recovery Practice Statement.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

The DoD PKI currently supports private encryption key escrow and recovery. The DoD PKI does not support key recovery using key encapsulation techniques.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

CAs and OCSP High Volume Responders shall consist of equipment dedicated to these CMA functions. It shall not perform non-CMA related functions.

Unauthorized use of CMA equipment is forbidden. Physical security controls shall be implemented that protect the CMA hardware and software from unauthorized use. CMA cryptographic modules shall be protected against theft, loss, and unauthorized use.

5.1.1 Site Location and Construction

The location and construction of the facility that will house CMA equipment and operations shall be in accordance with DoD and local policy for protecting information of the same value or classification as the material that will be protected by the public key certificates issued or managed there. See *Safeguarding Communications Security (COMSEC) Facilities and Material* [CNSS 4005] for information on protecting classified information.

5.1.2 Physical Access

With the exception of the FORTEZZA CAW, CA and OCSP Responder equipment and cryptographic modules shall always:

- be protected from unauthorized access; and,
- require the presence of at least two trusted role personnel (see Section 5.2.1) for any access to the CA or the OCSP Responder equipment or to the CA or the OCSP Responder cryptographic module.

FORTEZZA CAW and associated cryptographic modules shall always be protected from unauthorized access.

RA equipment shall be protected from unauthorized access while the cryptographic module is installed and activated. The RA shall implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms shall be commensurate with the level of threat in the RA equipment environment.

When not in use, removable CA and OCSP Responder cryptographic modules, and any activation information used to access or enable the cryptographic modules or equipment, shall be placed in locked containers sufficient for housing equipment and information commensurate with the classification, sensitivity, or value of the information being protected by the certificates issued by the CA. Activation data shall either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and shall not be stored with the cryptographic module.

A security check to the facility housing CA and OCSP Responder equipment shall occur prior to leaving the facility unattended. The check shall verify that:

- the equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open,” and secured when “closed”);
- any security containers are properly secured;
- physical security systems (e.g., door locks, vent covers) are functioning properly; and,
- the area is secured against unauthorized access.

A person or group of persons shall be made explicitly responsible for making such checks. When a group of persons are responsible, a log identifying the person performing a check at each instance shall be maintained. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

Facilities housing Medium Assurance or High Assurance CA and OCSP Responder equipment shall, if

unattended for periods greater than 24 hours, be protected by an intrusion detection system. Additionally, a check shall be made at least once every 24 hours to ensure that no attempts to defeat the physical security mechanisms have been made.

Current NSA policy requires that a hardware cryptographic module used for issuing certificates whose keys will protect classified information is classified at the level of that information, both when in use and when not in use. When not in use, it must be stored in a container approved for classified cryptographic storage, where access is allowed only to authorized CMA operators as defined in Section 5.2.

5.1.3 Power and Air Conditioning

The facility, which houses the CA equipment, shall be supplied with power and air conditioning sufficient to create a reliable operating environment.

The CA equipment shall have or be provided with sufficient back-up power to execute a standard shutdown (including locking out input, finishing any pending actions, and recording the state of the equipment) before lack of primary power or air conditioning causes the CA equipment to cease functioning. Subscribers or Relying Parties with needs for long operation hours or short response times may contract with a CA for additional requirements for backup power.

Power and air conditioning support to the repository that are the primary source of CA certificates and/or CRLs for access by relying parties shall be sufficient to ensure that availability requirements of Section 2.1 are met.

5.1.4 Water Exposures

CA equipment shall be installed such that it is not in danger of exposure to water, e.g., on tables or elevated floors. Moisture detectors shall be installed in areas susceptible to flooding. CA operators who have sprinklers for fire control shall have a contingency plan for recovery should the sprinklers malfunction or cause water damage outside of the fire area.

5.1.5 Fire Prevention and Protection

A description of the CMA's approach for recovery from a fire disaster shall be included in the Disaster Recovery Plan required by Section 5.7.4.

5.1.6 Media Storage

Media shall be stored so as to protect it from accidental damage (water, fire, electromagnetic). Media that contains sensitive information (e.g., identified in Section 9.4, security audit, archive, backup information shall be protected from unauthorized access.

5.1.7 Waste Disposal

Normal office waste shall be removed or destroyed in accordance with local policy. Media used to collect or transmit sensitive information (e.g., personal information identified in Section 9.4, security audit, archive, backup information) shall be destroyed, such that the information is unrecoverable, prior to disposal.

5.1.8 Off-Site Backup

System backups, sufficient to recover from system failure, shall be made on a periodic schedule. For Medium and High Assurance CAs that are continuously operated (for periods of one week or longer), full system backups shall be performed once a week. For intermittently operated Medium Assurance and High Assurance CAs, the full system backup shall be performed each time the system is turned on or once a week, whichever is less frequent. At least one backup copy shall be stored at an offsite location (separate from the CA equipment). Only the latest backup need be retained. The backup shall be stored at a site with physical and procedural controls commensurate to that of the operational CA system.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles must be diligent and trustworthy as described in the next section. The functions performed in these roles form the basis of trust in the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first approach is to ensure that the person filling the role is trustworthy and properly trained. The second is to distribute the functions of the role among several people, so that any malicious activity requires collusion. Requirements regarding the design and configuration of the technology to avoid mistakes and counter inappropriate behavior are described in Section 6.

The primary trusted roles defined by this policy are the CA, the OCSP Responder, and the RA.

5.2.1.1 Certificate Authority

All certificates asserting a DoD certificate policy must be issued by a CA facility operating under the control of a CA. The responsible person or body (e.g., board of directors) identified as the facility's CA must be named, and made available during compliance audits.

Any CA who asserts a policy identifier defined in this document is subject to the stipulations of this policy. The CA's role and the corresponding CA procedures shall be defined in a CPS. Primarily, the CA's responsibilities are to ensure that the following functions occur according to the stipulations of this policy:

- RA functions as described in Section 5.2.1.2, if no separate RA is employed;
- certificate generation and revocation;
- posting certificates and CRLs;
- performing the incremental database backups;
- administrative functions such as compromise reporting and maintaining the database; and,
- hardware cryptographic module programming and management, if appropriate.

5.2.1.2 Registration Authority

Any RA, which operates under this policy, is subject to the stipulations of this policy, and of the PMA approved CPS under which it operates. Primarily, an RA's responsibilities are:

- verifying identity, pursuant to Section 3.2.3;
- entering Subscriber information, and verifying correctness;
- securely communicating requests to and responses from the CA; and,
- receiving and distributing Subscriber certificates.

The RA role is highly dependent on public key infrastructure implementations and local requirements. The responsibilities and controls for RAs shall be explicitly described in the CPS of a CA if the CA uses an RA.

5.2.1.3 Other Trusted Roles

For Medium Assurance and High Assurance infrastructures, a CMA shall, in its CPS, define other trusted roles to which shall be allocated responsibilities that ensure the proper, safe, and secure operation of the CMA equipment and procedures. These responsibilities include:

- System Administrator: initial configuration of the system; including installation of applications; initial setup of new accounts; configuration of initial host and network interface; assignment of security privileges and access controls for accounts and other trusted roles; creation of devices to support recovery from catastrophic system loss; performance of system backups, software upgrades and recovery; perform secure storage and distribution of the backups and upgrades to an off-site location; change of the host or network interface configuration;
- Compliance Auditor: performance of compliance audit; and,

- ISSO: performance of archive and deletion functions of the security audit log and other archive data as described in Sections 5.4 and 5.5 of this document; review of the security audit log.

To ensure system integrity, the CMAs shall be prohibited from performing these responsibilities for their own CMA facility. The CMA shall maintain lists, including names, organizations, and contact information, of those who act in these trusted roles, and shall make them available during compliance audits.

5.2.1.4 PKI Sponsor

A PKI Sponsor fills the role of a Subscriber for non-human system components and organizations (including groups and roles) that are named as public key certificate subjects. The PKI Sponsor works with the CMAs and (when appropriate) their TAs to register components (e.g., routers, firewalls) in accordance with Section 3.2.3.3, and is responsible for meeting the obligations of Subscribers as defined throughout this document.

5.2.1.5 Online Certificate Status Protocol (OCSP)

Any OCSP Responder, which operates under this policy, is subject to the stipulations of this policy, and of the PMA approved CPS under which it operates. Primarily, an OCSP Responder is responsible for:

- Providing certificate revocation status to the relying parties; and,
- Ensuring that the revocation status responses contain authentication and integrity services commensurate with the assurance level of the certificate being checked.

5.2.2 Number of Persons Required for Task

Requirements for multi-person control is described in Section 6.2.2.

5.2.3 Identification and Authentication for Each Role

Person occupying a trusted role shall authenticate himself to the local system in accordance with *Information Assurance (IA) Implementation* [DoDI 8500.2].

Person occupying a trusted role shall authenticate to a remote infrastructure component of the DoD PKI using a valid DoD X.509 certificate.

5.2.4 Roles Requiring Separation of Duties

Under no circumstances shall the incumbent of a CMA role perform its own compliance or security auditor function. A Compliance Auditor shall not perform any other role on the CMA. Except in the FORTEZZA PKI, an ISSO shall not perform any other role on the CMA. A CMA shall not perform any role on the CA, including being the ISSO or the compliance auditor. An RA shall not perform system administrator/ISSO duties on any system where they exercise CMA authority.

The CA, RA and OCSP Responder software and hardware shall enforce these role separations.

No individual shall have more than one identity on any CA, RA or OCSP Responder system.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

Persons shall be selected for any CMA or other trusted role on the basis of loyalty to the United States, their trustworthiness, and integrity. CMAs may be US uniformed service members or government civilian employees of any organization authorized by the PMA to possess and issue DoD PKI certificates in accordance with Section 1.3.3 of this CP, or such organizations' contractors. All CMAs shall be US citizens. All persons filling trusted roles other than CMAs shall be US citizens or hold a US security clearance.

All CA operations, and OCSP High Volume Responders, shall be administered by a person or body (e.g., a Board of Directors). This person or body shall be identified as the CA or OCSP Responder as described in Sections 1.3, 1.3.1, 1.3.2, 5.2.1.1, and 5.2.1.5. High Assurance CAs and OCSP High Volume Responders shall be administered by a military commissioned or warrant officer, government employee GS-7 or above, or

a civilian contractor/vendor employee of equivalent or greater responsibility and compensation. The operators and equipment for a CA and OCSP High Volume Responder installation must be within the administrative control of the identified administrator.

Personnel appointed to operate CMA equipment within the DoD PKI may be military, civilian, or contractor personnel and shall:

- have successfully completed an appropriate training program;
- have demonstrated the ability to perform their duties;
- be trustworthy;
- have no other duties that would interfere or conflict with their duties as a CMA;
- have not been previously relieved of CMA or COMSEC custodian duties for reasons of negligence or non-performance of duties;
- have not been denied a security clearance, or had a security clearance revoked;
- have not been convicted of a felony offense; and,
- be appointed in writing by an approving authority, or be party to a contract for PKI services.

CMAs issuing or requesting certificates asserting security clearances (e.g., Confidential, Secret, Top Secret) shall hold a security clearance equal to or higher than the clearance being asserted. CMAs need not themselves hold other authorizations asserted in the certificates (e.g., security categories), unless the policy associated with these authorizations so requires.

5.3.2 Background Check Procedures

Local service, agency, or community procedures shall be followed to determine the type of background check to be performed. Such checks are to be performed solely to determine the suitability of a person to fill a PKI role, and shall not be released except as required in Section 9.3. Background check procedures shall be described in the CPS.

5.3.3 Training Requirements

All personnel involved in the CMA operation shall be appropriately trained. Topics shall include the operation of the CMA software and hardware, operational and security procedures, and the stipulations of this policy and local guidance. The specific training required will depend on the equipment used and the personnel selected. A training plan shall be established for a CMA installation, and training completed by the personnel shall be documented.

5.3.4 Retraining Frequency and Requirements

Those involved in filling PKI roles shall be aware of changes in the CMA operation. Any significant change to the CMA operation shall have a training (awareness) plan, and the execution of such plan shall be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of CA equipment.

5.3.5 Job Rotation Frequency and Sequence

This policy makes no stipulation regarding frequency or sequence of job rotation. Local policies, which do impose requirements, shall provide for continuity and integrity of the PKI service.

5.3.6 Sanctions for Unauthorized Actions

A CMA shall take appropriate administrative and disciplinary actions against personnel who violate this policy.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to operate any part of the PKI shall be subject to the same criteria as a US Government employee, and cleared to the level of the information protected by the certificates the PKI issues.

PKI vendors who provide services to the DoD shall establish procedures to ensure that any subcontractors perform in accordance with its CPS and this policy.

5.3.8 Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each role shall be provided to the personnel filling that role.

5.4 AUDIT LOGGING PROCEDURES

This section describes the security audit requirements for CMAs.

5.4.1 Types of Events Recorded

Requirements applied to CA, OCSP Responder and RA equipment:

Any security auditing capabilities of the underlying CMA equipment operating system shall be enabled during installation.

At a minimum, the following CMA events shall be recorded:

- CMA application access (e.g., logon);
- messages received from any source requesting CMA actions (certificate requests, certificate signing, certificate revocation, compromise notification); OCSP Responders are exempt from this audit requirement;
- actions taken in response to requests for CMA actions; for OCSP Responders, a CMA ISSO shall record the results of the analysis of a weekly sample of responses sent by each responder;
- physical access to, loading, zeroizing, transferring keys to or from, backing-up, acquiring or destroying CMA cryptographic modules;
- receipt, servicing (e.g., keying or other cryptologic manipulations), and shipping hardware cryptographic modules;
- posting of any material to a repository;
- anomalies, error conditions, software integrity check failures, receipt of improper or misrouted messages; and,
- any known or suspected violations of physical security, suspected or known attempts to attack the CMA equipment via network attacks, equipment failures, power outages, network failures, or violations of this certificate policy.

The CA equipment and OCSP High Volume Responders shall record server installation, access, and modification (to include changes in configuration files, security profiles, administrator privileges).

For Medium Assurance and High Assurance, the following must be recorded for CAs and OCSP High Volume Responders:

- equipment access (e.g., room access);
- file manipulation and account management;
- posting of any material to a repository;
- access to databases; and,
- any use of the signing key.

For each auditable event defined in this section, the CMA security audit record shall include, at a minimum:

- the type of event;
- the time the event occurred;
- for messages from RAs (or other entities) requesting CA actions, the message source, destination and contents;
- for attempted CA certificate signature or revocation – a success or failure indication; and,
- for operator initiated actions (including equipment and application access), the identity of the equipment operator who initiated the action.

Where possible, the security audit data shall be automatically collected; when this is not possible a logbook, paper form, or other physical mechanism shall be used. All security audit logs, both electronic and non-electronic, shall be retained in accordance with the requirements of Section 5.4.3.

5.4.2 Frequency of Processing Log

For Medium Assurance, at least 6 periodic reviews are required per year, with a minimum of 25 percent of the security audit data generated since the last review to be examined.

For High Assurance, at least 12 (monthly) reviews are required per year, with at least 33 percent of the security audit data generated since the last review to be examined.

The CMA shall implement procedures to ensure that the security audit data is transferred prior to overwriting or overflow of automated security audit log files.

5.4.3 Retention Period of Audit Log

The information generated on the CMA equipment shall be kept on the CMA equipment until the information is removed and stored as specified in Section 5.4.4. Deletion of the security audit data from the CMA equipment shall be performed by an entity other than the CMA. This entity shall be identified in the CMA's CPS. Security audit data shall be available on-site for at least two months or until reviewed, then off-site as archive records in accordance with Section 5.5.2. All security audit logs, both electronic and non-electronic, shall be retained and made available during compliance audits.

5.4.4 Protection of Audit Log

The security audit data shall not be open for reading or modification by any human, or by any automated process other than those that perform security audit processing. CMA system configuration and procedures must be implemented together to ensure that only authorized people archive or delete security audit data. The entity performing security audit data archive need not have ‘Modify’ access, but procedures must be implemented to protect archived data from deletion or destruction prior to the end of the security audit data retention period (note that deletion requires modification access). Security audit data shall be moved to a safe, secure storage location separate from the CMA equipment.

5.4.5 Audit Log Backup Procedures

Security audit data shall be backed up at least monthly. A copy of the security audit data shall be sent off-site on a monthly basis as specified in the CPS.

5.4.6 Audit Collection System (Internal vs. External)

The security audit process shall run independently and shall not in any way be under the control of the CMA. Operating system security audit processes shall be invoked at system startup, and cease only at system shutdown. All application security audit processes shall be invoked at system startup and cease only at application shutdown. Should it become apparent that an automated security audit system has failed, the CMA shall cease all operation except for revocation processing until the security audit capability can be restored. Under these circumstances, the CMA shall employ mechanisms to preclude unauthorized CMA functions. These mechanisms shall be described in the CMA's CPS.

5.4.7 Notification to Event-Causing Subject

There is no requirement to notify a subject that an event was audited. Real-time alerts are neither required nor prohibited by this policy.

5.4.8 Vulnerability Assessments

The CMA, system administrator, and other operating personnel shall be watchful for attempts to violate the integrity of the certificate management system, including the equipment, physical location, and personnel. The security audit data shall be reviewed by the security auditor for events such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses. Security auditors shall check for continuity of the security audit data. The ISSO shall document the summary results of the period review of the audit logs.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

CMA archive records shall be sufficiently detailed as to verify that the PKI was properly operated as well as verify the validity of any certificate throughout its validity period (e.g., valid, revoked, suspended). At a minimum, the following data shall be archived.

During CMA system initialization:

For all assurance levels:

- CMA accreditation (if necessary);
- CPs, CPSs;
- any contractual or other agreements to which the CMA is bound or that concern operations;
- Compliance Audit Reports; and,
- system equipment configuration.

During CMA operation:

For Medium Assurance and High Assurance:

- modifications or updates to any of the above data items;
- certificate requests and revocation requests;
- Subscriber identity authentication documentation as required by Section 3.2.3;
- documentation of receipt and acceptance of certificates as described in Section 4.4;
- documentation of receipt of tokens as described in Section 3.2.1;
- all certificates and CRLs (or other revocation information) as issued or published;
- security audit data (in accordance with Section 5.4);
- other data or applications sufficient to verify archive contents; and,
- all work related communications to or from the PMA, other CMAs, and compliance auditors.

5.5.2 Retention Period of Archive

Archive records covered by either a General Records Schedule established by the National Archives and Records Administration or an agency-specific schedule as applicable shall be retained as specified in the approved records schedule in accordance with *DoD Records Management Program* [DoDD 5015.2]. Otherwise, archive records shall be kept, without any loss of data, for a period of:

- at least ten years, six months for Medium Assurance;
- at least twenty years, six months for High Assurance;
- at least eleven years for the FORTEZZA/CAW PCA;
- at least eleven years for the FORTEZZA/CAW ICRLA; and,
- at least until decommission of the FORTEZZA/CAW PKI CA plus one year.

Applications necessary to read these archives must be maintained for at least the applicable retention period above.

The CMA shall maintain the archived data, or provide archived data and the applications necessary to read the archives to a PMA approved DoD archival facility, which shall retain the applications necessary to read this archived data, until expiration of the designated archive period.

The FORTEZZA PKI CA shall maintain the archived data, or provide archived data and the applications necessary to read the archives to the Service/Agency archival facility, which shall retain the applications necessary to read this archived data, until expiration of the designated archive period.

5.5.3 Protection of Archive

No unauthorized CMA equipment operator shall be able to modify or delete the archive, but archived records may be moved to another medium. If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media shall be defined by the archive site. No transfer of medium shall invalidate CMA applied signatures. The CMA shall maintain a list of people authorized to modify or delete the archive, and make this list available during CP compliance audits. Release of sensitive archive information will be as described in Section 9.4.

Archive media shall be stored in a separate, safe, secure storage facility. Prior to archive, archive records shall be labeled with the CMA's distinguished name, the date, and the classification.

5.5.4 Archive Backup Procedures

No stipulation.

5.5.5 Requirements for Time-Stamping of Records

No stipulation.

5.5.6 Archive Collection System (Internal vs. External)

Archive data may be collected in any expedient manner.

5.5.7 Procedures to Obtain and Verify Archive Information

Procedures detailing how to create, package, and send the archive information shall be published in a CMA procedures handbook or CPS. Only authorized CMA equipment operators will be allowed to access the archive.

5.6 KEY CHANGEOVER

A CA uses a signing (private) key for creating certificates; however, relying parties employ the CA certificate for the life of the Subscriber certificate beyond that signing. Therefore, CAs must not issue Subscriber certificates that extend beyond the expiration dates of their own certificates and public keys, and the CA certificate validity period must extend one Subscriber certificate validity period (listed in Section 3.3) past the last use of the CA private key. To minimize risk to the PKI through compromise of a CAs key, the private signing key will be changed more frequently, and only the new key will be used for certificate signing purposes from that time. The older, but still valid, certificate will be available to verify old signatures until all of the Subscriber certificates signed under it have also expired. If the old private key is used to sign CRLs that contain certificates signed with that key, then the old key must be retained and protected. For a thorough discussion of key changeover, see *Internet X.509 Public Key Infrastructure Certificate Management Protocol* [RFC 4210].

The following table summarizes in years the maximum validity period of the CA's signature certificate, and the maximum lifetime of the associated authority-signing key (used for certificate signing), separated by a slash. RA key lifetimes are as described for Subscribers in Section 3.3. If a CA certificate and key lifetime are selected that are shorter than a Subscriber's, then the RA certificate and key lifetime shall be no longer than that of the CA. Note that signature keys that have expired for the purposes of certificate signing may still be used for CRL signature. All values are in years.

Assurance Level	CA	Auto Issuance CA*	Intermediate CA	Root CA
Medium Assurance	6/3	6/6	10/4	36/20
High Assurance	6/3	6/6	10/4**	36/20**

* The Auto Issuance CA column refers to CAs that only use an automated process to issue certificates to non-human system components.
** FORTEZZA High Assurance PKI PCA and PAA is 11/5 and 36/25, respectively.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

If a hacking attempt or other form of potential compromise of a CA becomes known, it shall be investigated in order to determine the nature and the degree of damage. If the CA key is suspected of compromise, the procedures outlined in Section 5.7.3 shall be followed. Otherwise the scope of potential damage shall be assessed in order to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised.

In case of an OCSP Responder key compromise, a CA that issued the OCSP Responder a certificate, shall revoke that OCSP Responder s certificate, and the revocation information shall be published immediately in the most expeditious manner. Subsequently, the OCSP Responder shall be re-keyed.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

The CA shall maintain backup copies of system, databases, and private keys in order to rebuild the CA capability in case of software and/or data corruption. Prior to resuming operations, the CA shall ensure that the system's integrity has been restored.

5.7.3 Entity Private Key Compromise Procedures

In case of a CA key compromise, a superior CA shall revoke that CA's certificate, and the revocation information shall be published immediately in the most expedient manner. Subsequently, the CA installation shall be re-established as in Section 5.7.4. If the CA is a Root CA, the trusted self-signed certificate must be removed from each Relying Party application, and a new one distributed via secure out-of-band mechanisms. Root CAs shall describe their approaches to reacting to a Root CA key compromise in their CPSs.

5.7.4 Business Continuity Capabilities After a Disaster

Medium Assurance and High Assurance CAs are required to maintain a Designated Approving Authority (DAA) approved Disaster Recovery Plan.

In the case of a disaster in which the CA equipment is damaged and inoperative, the CA operations shall be reestablished as quickly as possible, giving priority to the ability to revoke Subscriber's certificates. If the CA cannot reestablish revocation capabilities prior to the shorter of the next update field in the latest CRL issued by the CA or one week, then the CA must report to the PMA. The PMA, shall decide whether to declare the CA private signing key as compromised, and reestablish the CA keys and certificates, all cross-certificates, and all Subscriber certificates, or allow additional time for reestablishment of the CA's revocation capability.

In the case of a disaster whereby a CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the CA shall request that its certificates be revoked. The CA installation shall then be completely rebuilt, by reestablishing the CA equipment, generating new private and public keys, being re-certified, and re-issuing all cross certificates. Finally, all Subscriber certificates shall be re-issued. In such events, any Relying Parties who continue to use certificates signed with the destroyed private key do so at their own risk and the risk of others to whom they forward data.

5.8 CA OR RA TERMINATION

See Section 9.10.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

All keys and intermediate keys and pseudo-random numbers used for all key generation shall be generated using a FIPS approved method. For example, a prime number for use with the RSA algorithm defined in RSA Cryptography Standard [PKCS 1] shall be generated and checked in accordance with [PKCS 1]. A private key is considered to be generated by the PKI entity that first comes into possession of it: a Subscriber, an RA, or a CA.

Random numbers for High Assurance key material shall be generated in FIPS 140 Level 2 validated hardware cryptographic module.

A private key must not appear outside of the module in which it was generated unless it is encrypted for transport (see Section 6.2.6) or for processing or storage by a key recovery mechanism.

CA cryptographic keying material shall be generated in FIPS 140 Level 2 validated hardware cryptographic modules.

The CA key generation shall be under two-person control. The procedures used to generate the CA keys shall be documented and signed by two or more individuals to provide auditable evidence that the documented procedures were followed. The documentation of the procedure shall be detailed enough to show that appropriate role separation was used. Independent third party (e.g., compliance auditor) shall validate the key generation procedures either by witnessing or by examining the signed and documented procedures.

OCSP Responder cryptographic keying material shall be generated in FIPS 140 Level 2 validated cryptographic modules. A FIPS 140 Level 2 validated hardware cryptographic module shall be used for OCSP High Volume Responders.

Medium Assurance key pairs shall be generated in FIPS 140 Level 1 validated cryptographic modules.

Medium Assurance Hardware and High Assurance signature key pairs shall be generated on the Subscriber token which shall be a FIPS 140 Level 2 validated hardware cryptographic module. High Assurance FORTEZZA CAW sites may generate signature public/private key pairs on behalf of a Remote User/Subscriber. Such key pairs will be generated only on a FIPS 140 Level 2 or higher FORTEZZA PCMCIA card or T2CSS board. If the key pair is to be extracted from the token on which it was generated (other than as per Section 6.2.2) for transmission to the Remote User/Subscriber or insertion into Type 2 Cryptographic Support Server (T2CSS), the keys must be securely extracted in a manner that guarantees that only the proper Remote User/Subscriber token can decrypt and access the new signature key. The module on which the key pair was generated must be immediately zeroized after extraction, and an approved process must be in place to ensure that no additional copies of the key can be made.

Medium Assurance Hardware encryption key pairs shall be generated in FIPS 140 level 2 validated hardware cryptographic modules. The key pairs may be generated off the token as long as there are assurances that no copies other than authorized key escrow copies of the keys continue to exist after the generation and insertion processes have completed.

High Assurance encryption key pair shall be generated on a FIPS 140 Level 2 validated hardware cryptographic module. The hardware module need not be the Subscriber token as long as there are assurances that no copies other than the authorized key escrow copy of the private encryption key continue to exist after the generation and transfer processes have completed.

6.1.2 Private Key Delivery to Subscriber

In most cases, a private key will be generated and remain within the cryptographic boundary of a cryptographic module. If the owner of the module generates the key locally, then there is no need to deliver the Subscriber's private key. If the key is generated on a hardware cryptographic module elsewhere, then the hardware cryptographic module must be delivered to the Subscriber. Accountability for the location and state of the hardware cryptographic module must be maintained until the Subscriber is in possession of it. The Subscriber shall acknowledge receipt of the hardware cryptographic module.

Private keys associated with medium assurance (excluding medium hardware) certificates may be generated and stored in software cryptographic modules. When the Subscriber generates these keys locally, there is no need to deliver them. If the private keys are generated elsewhere, they must be transmitted or delivered to the Subscriber in encrypted form and the encryption method ensures that only the Subscriber may possess the plaintext private signature keys. The encryption must be of strength commensurate with that of the key being protected. The Subscriber shall acknowledge receipt of the private signature key. The originally generated private signature key shall be destroyed. Mechanisms shall ensure that additional copies of software keys are not maintained except as allowed in this Certificate Policy.

Only those authorized by the DoD key recovery policy may access private keys associated with encryption certificates.

For all assurance levels, when keyed hardware tokens are delivered to Subscribers, the delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers. The CMA must maintain a record of receipt of the token by the Subscriber. When any mechanism that includes a shared secret (e.g., a password or Personal Identification Number (PIN)) is used, the mechanism shall ensure that the applicant and the CMA are the only recipients of this shared secret.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys shall be delivered to the certificate issuer in a way that binds the applicant’s verified identification to the public key being certified. This binding shall be accomplished using means that are as secure as the security offered by the keys being certified. The binding shall be accomplished using cryptographic, physical, procedural, and other appropriate methods. The methods used for public key delivery shall be stipulated in the CPS.

In those cases where public/private key pairs are generated by the CMA on behalf of the Subscriber, the CMA shall implement secure mechanisms to ensure that the token on which the public/private key pair is held is securely sent to the proper Subscriber, and that the token is not activated prior to receipt by the proper Subscriber.

As noted in Section 6.1.1, the FORTEZZA CAW may securely extract public/private key pairs from the token on which they were generated for transmission to a remote User/Subscriber. In such cases the protection mechanisms applied to the extracted keys shall also be in accordance with Section 6.2.6, and the certificate shall not be activated prior to receipt by the proper Remote User/Subscriber.

6.1.4 CA Public Key Delivery to Relying Parties

The PKI and the relying parties must work together to ensure the authenticated and integral delivery of Trusted Certificates. Acceptable methods for Trusted Certificate delivery include, but are not limited to:

- CAs or RAs loading Trusted Certificates onto tokens delivered to relying parties via secure mechanisms;
- secure distribution of Trusted Certificates through secure out-of-band mechanisms;
- comparison of certificate hashes or fingerprints against Trusted Certificate hashes or fingerprints made available via authenticated out-of-band sources (note that fingerprints or hashes posted in-band along with the certificate are not acceptable as an authentication mechanism); and,
- loading certificates from web sites secured with a currently valid DoD certificate of equal or greater assurance level than the certificate being downloaded.

Systems using High Assurance certificates shall store Trusted Certificates such that unauthorized alteration or replacement is readily detectable.

6.1.5 Key Sizes

For the FORTEZZA High Assurance PKI, Digital Signature Standard (DSS) keys issued by a US DoD PKI shall use at least 160-bit private key (x) and at least 1024 bit prime modulus (p). Minimum Subscriber public key sizes shall be 1024 bits for Key Exchange Algorithm (KEA).

For Medium Assurance (except Medium-2048, Medium Hardware-2048, and PIV-Auth-2048), Rivest, Shamir, Adleman (RSA) keys issued by the DoD PKI shall be 1024 bits. The Root CA key size shall be 2048 bits. (This shall not require DoD Root 1 to be revoked but DoD Root 1 shall only use its signing key for CRL issuance.) The minimum public key size for all Medium-2048, Medium Hardware-2048 and PIV-Auth-2048 RSA keys shall be 2048 bits. The minimum public key size for High Assurance RSA keys shall be 2048 bits. All RSA keys issued after 31 December 2010 shall be 2048 bits. OCSP responders shall sign responses using a signature algorithm, key size, and hash algorithm of equal or greater cryptographic strength than that used by the CA to sign CRLs.

For Medium Assurance, Elliptic Curve Cryptography Algorithm key prime field (*//p//*) shall be not less than 224, and the Binary Field (*m*) shall be not less than 233. For High Assurance, Elliptic Curve Cryptography Algorithm key prime field (*//p//*) shall be not less than 384, and the Binary Field (*m*) shall be not less than 409.

Use of SSL or another protocol for communication of registration information or private key delivery shall require, at a minimum, use of a symmetric key length and algorithm of workfactor equal to or greater than the workfactor associated with the Subscriber key pairs.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters shall always be generated and checked in accordance with the standard that defines the cryptoalgorithm in which the parameters are to be used. For example, public key parameters for use with algorithms defined in the *Digital Signature Standard* [FIPS 186-2] shall be generated and tested in accordance with [FIPS 186-2].

Whenever a cryptoalgorithm is described in [FIPS 186-2], the parameter generation and checking requirements and recommendations of [FIPS 186-2] shall be required of all entities generating key pairs whose public components are to be certified by the DoD PKI.

6.1.7 Key Usage Purposes (as per X.509 V3 Key Usage Field)

Public keys that are bound into certificates which assert the Medium Assurance or High Assurance policies shall be certified for use in signing or encrypting, but not both. The use of a specific key is determined by the key usage extension in the X.509 certificate. This restriction is not intended to prohibit use of protocols (like the Secure Sockets Layer) that provide authenticated connections using encryption certificates. Formats of the CA and end entity certificates, including how the *keyUsage* extension is populated in these certificates, are described in *DoD PKI Functional Interface Specification and Recomendations* [INT-SPEC].

Subscriber public keys that are bound into certificates which assert PIV-Auth or PIV-Auth-2048 Assurance shall assert a key usage extension of “digitalSignature” and shall not assert any other key usage extension.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is *Security Requirements for Cryptographic Modules* [FIPS 140, current version]. The PMA may determine that other comparable validation, certification, or verification standards are sufficient. These standards will be published by the PMA. Cryptographic modules shall be validated to the [FIPS 140] level identified in this section, or validated, certified, or verified via one of the standards published by the PMA.

Subscribers who have keys certified under Medium Assurance shall use cryptographic modules, which meet at least the criteria specified for Level 1. Subscribers who have keys certified under Medium Assurance Hardware shall use hardware cryptographic modules, which meet at least the criteria specified for Level 2. High Assurance certificates require Level 2 hardware cryptographic modules. A higher level may be used if available or desired. A PKI should provide the option of using any acceptable cryptographic module to facilitate the management of Subscriber certificates.

Both Medium Assurance and High Assurance certificates shall be signed using a hardware cryptographic module that meets Level 2.

OCSP Low Volume Responders may use hardware or software cryptographic modules for OCSP Responder key generation and protection, validated at FIPS 140 Level 2 or higher. All OCSP High Volume Responders shall use FIPS 140 Level 2 or higher hardware cryptographic modules.

Medium Assurance and High Assurance RAs use hardware cryptographic modules at Level 2.

All cryptographic modules shall be operated such that the private asymmetric cryptographic keys shall never be output in plaintext. No private key shall appear unencrypted outside the CA equipment.

No one shall have access to a private signing key but the Subscriber. Private decryption keys shall only be held by parties authorized by [KRP]. These keys shall be held in the strictest confidence and controlled as described in [KRP].

Private keys used to sign certificates that will assert security privileges are classified at the same level as the classification asserted in the certificate. In the case where the CA will not independently verify security privilege information, this requirement extends to RA private keys.

Note that Section 6.1.1 stipulates cryptographic module requirements for key generation.

Medium Assurance	Subscriber	RA and CA	OCSP Responder
FIPS 140 (current version) validation	Level 1	Level 2 (hardware)	Level 2*
Operational requirement	Shall not output private asymmetric key in plaintext		

Medium Assurance Hardware	Subscriber	RA and CA	OCSP Responder
FIPS 140 (current version) validation	Level 2 (hardware)	Level 2 (hardware)	Level 2*
Operational requirement	Shall not output private asymmetric key in plaintext		

High Assurance	Subscriber	RA and CA	OCSP Responder
FIPS 140 (current version) validation	Level 2 (hardware)	Level 2 (hardware)	Level 2*
Operational requirement	Shall not output private asymmetric key in plaintext		

* Level 2 (hardware) required for OCSP High Volume Responders.

6.2.2 Private Key (n out of m) Multi-Person Control

For FORTEZZA CAW, the CA may have single-person control of the CA Signing key. For all other CAs, key generation, key activation and key backup shall require the presence of two trusted roles as defined in Section 5.2.1. For these activities, one of the trusted roles shall be a system administrator. The other party shall not hold the ISSO or Compliance Auditor role.

For OCSP High Volume Responders, key generation, key activation and key backup shall require the presence of two trusted roles as defined in Section 5.2.1.

Access to CA or OCSP Responder signing keys backed up for disaster recovery shall be under at least two-person control.

The CA or OCSP Responder certificate request (including the public key generation and delivery) for the purpose of generating a CA or OCSP certificate shall be carried out under two-person control.
The names of the parties used for two-person control shall be maintained on a list that shall be made available for inspection during compliance audits.

6.2.3 Private Key Escrow

CA Private keys shall never be escrowed.

Under no circumstances shall a key used to support non-repudiation services be held in trust by any party other than the Subscriber.

For some purposes (such as data recovery) it shall be necessary to provide key retrieval for the private component of the encryption certificate key pair. To facilitate this, the PKI shall provide a key escrow capability.

The method, procedures and controls which will apply to the storage, request for, extraction and/or retrieval, delivery, protection and destruction of the requested copy of an escrowed key shall be described in a Key Recovery Policy (KRP) which shall become an integral component of this CP.

6.2.4 Private Key Backup

For Medium Assurance, Subscribers are permitted to back-up their own encryption (but not signature) private keys. Backup of a Subscriber's private signature keys for the sole purpose of key recovery shall not be made. Subscribers are permitted to make operational copies of private keys residing in software cryptographic modules for each of the Subscriber's applications or locations that requires the key in a different location or format. Medium Assurance, except for Medium Assurance Hardware, Component PKI Sponsors (see Sections 3.2.3 and 5.2.1.4) are authorized to make a single backup copy of the component private keys to support backup in cases where component malfunction results in key corruption. All key transfers shall be done from an approved cryptographic module, and the key shall be encrypted during the transfer. The Subscriber (PKI Sponsor for Components) is responsible for ensuring that all copies of private keys, including those that might be embedded in component backups, are protected including protecting any workstation on which any of its private keys reside.

A CA may only copy a Subscriber's hardware cryptographic module in response to a valid initial request for a backup, or as a result of an administrative action form request signed by the Subscriber. Every access authorization shall be documented, and each resultant access recorded. Only CAs and Subscribers shall back-up private keys (RAs shall not back-up private keys).

Backup copies of CA private signature keys shall only be made and handled under the same multi-person control as the original signature key. No more than two backup copies of the CA private signature keys may be made. One copy of the backup shall be kept at a backup location.

OCSP Responder's private signature keys shall be backed up as defined in Section 5.6. No more than two backup copies of the OCSP Responder's private signature keys may be made. If backups are made, only a single copy of any signature key is to be kept at the OCSP Responder location; if a second copy is made, it shall be kept at a backup location. The backup module shall also meet the cryptographic module requirements for the OCSP Responder.

The High Assurance FORTEZZA CAW sites may require backup CA material to comply with Disaster Recovery Plans and other instances requiring additional backup CA material. The DoD Policy Creation Authority (PCA) is authorized to create up to two copies of a CA key for a primary site and an additional copy for each of up to two approved backup sites, upon receipt of a valid request from the CAW site and approval by the Service or Agency CAW Approving Authority. The backup site locations need not be disclosed in the request. In addition, upon receipt of a valid request from the CAW site and approval by the Service or Agency CAW Approving Authority attesting to the non-functional status and destruction of one of the original

copies created, the PCA is authorized to create an additional replacement copy. Valid requests for CAW CA Materials in excess of the above-stated quantities shall additionally require PCA approval.

Neither RAs nor Subscribers shall back up High Assurance private keys.

6.2.5 Private Key Archival

See Sections 6.2.3 and 6.2.4.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

Private keys are to be generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key must be encrypted during transport; private keys must never exist in plaintext form outside the cryptographic module boundary. Transport of a private key must only be to an authorized entity (only the Subscriber in the case of a signature key) and the strength of the encryption must be at least commensurate with the key being transported.

Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure. The protection of these keys must be commensurate with that provided the data protected by the certificate associated with the private key.

6.2.7 Private Key Storage on Cryptographic Module

The private key stored in the cryptographic module shall be protected from unauthorized access and use in accordance with [FIPS 140] requirements applicable for the module.

6.2.8 Method of Activating Private Key

Pass-phrases, PINs, biometric data, or other mechanisms of equivalent authentication robustness must be used to activate the private key in a cryptographic module. (Activation data generation requirements are specified in Section 6.4.1.) Activation data may be distributed in person, or mailed to the Subscribers separately from the cryptographic modules that they activate. Entry of activation data must be protected from disclosure (e.g., the data should not be displayed while it is entered).

6.2.9 Method of Deactivating Private Key

Cryptographic modules, which have been activated, must not be left unattended or otherwise open to unauthorized access. After use, they must be deactivated, e.g., via a manual logout procedure, or by a passive timeout. Hardware cryptographic modules shall be removed and stored when not in use.

6.2.10 Method of Destroying Private Key

Private keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked. For software cryptographic modules, this can be overwriting the data. For hardware cryptographic modules, this will likely be executing a “zeroize” command. Physical destruction of hardware should not be required.

6.2.11 Cryptographic Module Rating

Requirements for cryptographic modules are as stated in Section 6.2.1.

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

The public key is archived as part of the certificate archival.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

Code signers and PIV content signers may use their private keys for up to 13 months; the lifetime of the associated public key certificates shall not exceed six years.

The key usage periods for keying material for other end entities are described in Section 3.3.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

Activation data may be Subscriber selected. A pass-phrase, PIN, biometric data, or other mechanisms of equivalent authentication robustness shall be used to protect access to use of a private key. Activation data shall meet the "strength of authentication mechanism" requirements in Section 4.4.3 of [FIPS 140].

Subscriber (to include CMAs) PINs, when used, shall be 6-8 digits at a minimum. Randomly generated PINs shall be used when possible. If this is not possible, Subscribers who create their own PINs shall be instructed to select PINs that are not related to their personal identity, history, or environment. Sequences, repeated numbers, social security numbers, and date formats, or other easily guessed numbers shall not be used. When alphanumeric pass-phrases are used, an interspersed mix of 8 characters, including at least two interspersed digits, shall be used. The activation data shall not resemble dictionary words; they shall differ from words or names by at least two characters that are not simple number-for-letter substitutions and shall not consist of words or names followed by 1-4 digits. The activation data shall not contain sequences, repeated characters, date formats, or license plate formats. To the extent practicable, technical means shall be used to verify that the activation data meets all of the requirements in this section.

If random numbers are used to generate PINs or pass-phrases, they shall meet all the applicable [FIPS 140] requirements. The method used to derive PIN or pass-phrase characters from the random numbers shall ensure that all valid characters for the PIN or pass-phrase are selected with equal probability (e.g., generate a random number (with 8 bits of entropy) and either use it if it corresponds to the ASCII representation of an element of the valid character set, or otherwise reject it and obtain an additional 8 bits of random data and repeat).

If the activation data must be transmitted, it shall be via a channel of appropriate protection, and distinct in time and place from the associated cryptographic module. If this is not done by hand, the Subscriber shall be advised of the shipping date, method of shipping, and expected delivery date of any activation data. As part of the delivery method, Subscribers will sign and return a delivery receipt. In addition, Subscribers should also receive (and acknowledge) a Subscriber advisory statement to help to understand responsibilities for use and control of the cryptographic module.

6.4.2 Activation Data Protection

Activation data for cryptographic modules should be memorized, not written down. If written down, it shall be secured at the level of the data that the associated cryptographic module is used to protect, and shall not be stored with the cryptographic module.

Activation data for private keys associated with certificates asserting individual identities shall never be shared. Activation data for private keys associated with certificates asserting organizational identities shall be restricted to those in the organization authorized to use the private keys.

6.4.3 Other Aspects of Activation Data

Medium Assurance and High Assurance CMAs shall change their CMA cryptographic module activation data whenever the CMA token is returned for maintenance or re-key.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

CA and OCSP Responder equipment used for Medium Assurance infrastructures shall use operating systems that:

- Require authenticated logins;
- Provide discretionary access control;

- Provide a security audit capability.
- Provide process isolation; and,
- Support recovery from key or system failure.

CA and OCSP Responder equipment used for High Assurance infrastructures shall be hosted on operating systems that implement the requirements of Medium Assurance, plus:

- Trusted path;
- CA application that was developed using Trusted System Development Methodology (TSDM) Level 2, was evaluated for compliance with Certificate Issuing & Management Component (CIMC) Protection Profile, Level 3, or a comparable PMA approved standard; and,
- OCSP Responder shall be evaluated for compliance with Common Criteria (CC) Evaluation Assurance Level (EAL) 4 or a comparable PMA approved standard.

When CA or OCSP Responder equipment is hosted on evaluated platforms in support of computer security assurance requirements then the system (hardware, software, and operating system) shall, when possible, operate in an evaluated configuration. At a minimum, such platforms shall use the same version of the computer operating system as received the evaluation rating.

6.5.2 Computer Security Rating

See Section 6.5.1.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

High Assurance CA applications shall be developed using Trusted System Development Methodology (TSDM) Level 2.

6.6.2 Security Management Controls

The CA and OCSP Responder equipment shall be dedicated to administering a key management infrastructure. The configuration of the CA and OCSP Responder systems, as well as any modifications and upgrades, shall be documented. The CA and OCSP Responder systems shall not have installed applications or component software, which are not part of the CA and OCSP Responder configuration. A formal configuration management methodology shall be used for installation and ongoing maintenance of CA and OCSP Responder systems. There shall be a mechanism for detecting unauthorized modifications to the CA and OCSP Responder system software or configuration.

Reasonable care shall be taken to prevent malicious software from being loaded on RA equipment. Only applications required to perform the organization's mission shall be loaded on the RA computer, and all such software shall be obtained from sources authorized by local policy. Data on RA equipment shall be scanned for malicious code on first use and periodically afterward.

6.6.3 Life Cycle Security Controls

Equipment (hardware and software) procured to operate a PKI shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with, such as random selection. Equipment developed for a PKI shall be developed in a controlled environment. For High Assurance, the development process shall be defined and documented.

All hardware and software that has been identified as supporting an OCSP High Volume Responder or a CA must be shipped or delivered via controlled methods that provide a continuous chain of accountability from the location where it has been identified as supporting a CMA function to the using facility. CA and OCSP Responder (for those OCSP Responders specified above in this paragraph) software, when first loaded, shall be verified as being that supplied by the authorized source, with no unauthorized modifications, and be the version intended for use.

Equipment updates shall be purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

For classified applications, the CA equipment and cards will be shipped via the COMSEC Material Control System (CMCS) if any classified application software has been loaded, or if any classified information has ever been loaded on the equipment or cards.

Medium Assurance	Purchase in manner to reduce likelihood of tampering, or develop in controlled environment; Protective packaging, accountable delivery method
High Assurance	Developed via documented controlled process; Tamper-evident packaging, controlled delivery method for CA equipment and end-entity cryptographic module

6.7 NETWORK SECURITY CONTROLS

CMA equipment shall be located on internal networks behind boundary/perimeter network defenses and afforded protections consistent with [DoDI 8500.2] policy for network security at the Mission Assurance Category I (MAC I) level. Services allowed to and from the Medium Assurance and High Assurance CA and OCSP Responder equipment shall be limited to those required to perform CMA functions. Other CMA equipment may enable additional services consistent with local policy.

Protection of CMA equipment shall be provided against known network attacks. All unused network ports and services shall be turned off. Any network software present on the CMA equipment shall be necessary to the functioning of the CMA application. Root CA equipment shall be stand-alone (off-line) configurations. Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment even if those services are enabled for other devices on the network.

6.8 TIME STAMPING

No stipulation.

7 CERTIFICATE, CSP, AND OCSP PROFILE

7.1 CERTIFICATE PROFILE

7.1.1 Version Number(s)

This policy governs only DoD X.509 Version 3 certificates. CMAs who issue or manage X.509 Version 1 certificates are subject to the *Information Systems Security Policy and Procedures for FORTEZZA Card Certification Authority Workstations* [NAG 69C].

Formats of the various certificates are described in [INT-SPEC].

7.1.2 Certificate Extensions

Rules for the inclusion, assignment of value, and processing of extensions are defined in profiles. These profiles are written to prescribe an appropriate amount of control over an infrastructure, yet be flexible enough to meet the needs of the various CAs and communities. High Assurance infrastructure shall use the extensions and path processing defined in *X.509 Certificate and Certificate Revocation List Profiles and Certification Path Processing Rules for MISSI* [SDN 706]. Medium Assurance infrastructures shall use *Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile* [FPKI-Prof]. Any variance to these profiles shall be approved by the DoD PKI Technical Working Group, and documented in a CPS. Whenever private extensions are used, they shall be identified in a CPS. Critical private extensions shall be interoperable in their intended community of use.

Access control information may be carried in the subjectDirectoryAttributes extension. If this is desired, the syntax is defined in detail in [SDN 702].

7.1.3 Algorithm Object Identifiers

Certificates under this Policy will use the following OIDs for signatures:

id-dsa-with-sha1	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
sha1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13}
id-RSASSA-PSS	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10}
ecdsa-with-SHA1	{iso(1) member-body(2) us(840) ansi-x9-62 (10045) signatures (4) 1}
ecdsa-with-SHA256	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2}
ecdsa-with-SHA384	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3}
ecdsa-with-SHA512	{iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4}

Where certificates are signed using RSA with PSS padding, the OID is independent of the hash algorithm; the hash algorithm is specified as a parameter. RSA signatures with PSS padding may be used with the hash algorithms and OIDs specified below:

id-sha256	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1}
id-sha512	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3}

Certificates under this Policy will use the following OIDs for identifying the algorithm for which the subject key was generated:

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
id-ecPublicKey	{iso(1) member-body(2) us(840) ansi-x9-62(10045) public key-type (2) 1}
id-ecDH	{iso(1) identified-organization(3) certicom(132) schemes(1) ecdh(12)}
rsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-keyExchangeAlgorithm	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22}

Where certificates contain an elliptic curve public key, the parameters shall be specified as one of the following named curves:

ansip256r1	{iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7}
ansip384r1	{iso(1) identified-organization(3) certicom(132) curve(0) 34}
ansip521r1	{iso(1) identified-organization(3) certicom(132) curve(0) 35}

In order to provide cryptographic separation for a closed community, when the subject public key is of the form id-ecDH, a private OID may be asserted to indicate a different base point on one of the above curves.

The DoD PKI shall certify only public keys associated with the cryptoalgorithms identified above, and shall only use the signature cryptoalgorithms described above to sign certificates, certificate revocation lists and any other PKI product.

7.1.4 Name Forms

In general, the DN will be used throughout the DoD X.500 Directories for lookups. All PKIs shall have the ability to generate and process DNs. Some communities or installations may choose to use other names, for example certificates used to implement a hardware protocol, where device addresses are most useful and certificate lookup is not performed. In this case, an alternate name form may be included in the subjectAltName extension. If there is no DN (all High Assurance certificates shall have a DN), then the subject field of the base certificate shall be an empty sequence, and that extension shall be marked critical. Any name form defining GeneralName in [ISO 9594-8] may be used, in accordance with the required profile (Section 7.1.2).

Use of alternate name forms shall be defined in a CPS, including criticality, types, and name constraints.

7.1.5 Name Constraints

CA certificates issued under a **High Assurance** PKI shall impose name constraints and path length constraints as required by [SDN 706].

7.1.6 Certificate Policy Object Identifier

Certificates issued under this policy shall assert the OID appropriate to the level of assurance with which it was issued, as defined in Section 1.2.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued under this policy shall not contain policy qualifiers.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

This policy does not require the certificatePolicies extension to be critical. Relying Parties whose client software does not process this extension risk using certificates inappropriately.

7.2 CRL PROFILE

7.2.1 Version Number(s)

CRLs issued under this Policy shall assert a version number as described in [ISO 9594-8]. High Assurance CRLs shall assert Version 2. Medium Assurance CRLs may assert Version 1 or Version 2.

7.2.2 CRL and CRL Entry Extensions

Detailed CRL profiles covering the use of each extension are available in [SDN 706]. Certificates issued by a Medium Assurance PKI may alternately conform to the profile recommendations in [FPKI-Prof], or may issue CRLs asserting no extensions. Any variance to these profiles shall be approved by the DoD PKI Technical Working Group, and documented in a CPS.

7.3 OCSP PROFILE

7.3.1 Version Number(s)

The DoD PKI shall use OCSP version 1.

7.3.2 OCSP Extensions

Appropriate extensions from [RFC 2560] may be used in OCSP requests and responses. If a request contains a nonce and the response does not contain the nonce, the Relying Party may process the response if the information is deemed reasonably current.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 FREQUENCY AND CIRCUMSTANCES OF ASSESSMENT

All CAs and OCSP High Volume Responders shall be audited on an annual basis, except for the CAW-based infrastructure, which shall be audited on a biennial basis.

The Services or Agencies shall also have the right to require periodic and aperiodic inspections of OCSP Responder operations to validate that the OCSP Responder is operating in accordance with the security practices and procedures described in its CPS. Additionally, all CAs have the right to require periodic and aperiodic inspections of subordinate CMA operations to validate that the subordinate CMA is operating in accordance with the security practices and procedures described in the subordinate's CPS. The CA will state the reason for any aperiodic inspection.

The PMA has the right to require aperiodic compliance audits of CMAs asserting this policy. The PMA shall state the reason for any aperiodic compliance audit. RAs and LRAs shall be audited aperiodically.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The auditor must demonstrate competence in the field of compliance audits and must be thoroughly familiar with the CMA's CPS. The compliance auditor must perform CA or Information System compliance audits as a primary responsibility. The CPS shall name the compliance auditor for each CMA.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The compliance auditor and audited party, shall have a contractual relationship for the performance of the compliance audit, or be sufficiently organizationally separated from the audited party to provide an unbiased, independent evaluation. To ensure independence and objectivity, the CA (except for FORTEZZA CAW) compliance auditor may not have served the entity in developing or maintaining the audited entity's facility or CPS.

8.4 TOPICS COVERED BY ASSESSMENT

The purpose of a compliance audit shall be to verify that the audited party has in place a system to assure the quality of the services that it provides, and that it complies with all of the requirements of this CP and its CPS. All aspects of the audited party's operation related to this CP shall be subject to compliance audit inspections.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

When the compliance auditor finds a discrepancy between a CMA's operation and the stipulations of its CPS, the following actions must occur:

- the compliance auditor shall note the discrepancy;
- the compliance auditor shall notify the parties identified in Section 8.6 of the discrepancy; and,
- the audited party or auditor will propose a remedy, including expected time for completion, to the DoD PKI PMO.

If the compliance auditor finds a critical failure that contributes to the ongoing compromise of sensitive information, the compliance auditor shall immediately report the issue to both the local authority (local base commander or ISSO) and the PMA Director, DoD PKI PMO (or CPMWG) to determine if the circumstances warrant the immediate shut down of operations, and/or the revocation of associated certificates. Such failures could include, but are not limited to: detection of a successful attempt to compromise sensitive information; detection of an overt and intentional disregard for secure operations of the system; detection of a system configuration that causes the wide-spread public dissemination of sensitive information.

The PMA will determine the appropriate remedy, up to and including revocation or non-recognition of the audited party's certificate. Upon correction of the deficiency, the PMA may reinstate the CMA.

8.6 COMMUNICATIONS OF RESULTS

The compliance auditor shall report the results of a CMA compliance audit to the PMA. The results will be reported to the audited CMA, and its superior CA if applicable, in accordance with Section 9.3. The implementation of remedies shall be communicated to the PMA. The PMA as the authorized party will determine the appropriateness of the remedy and may take additional measures as defined in Section 8.5. A special compliance audit may be required to confirm the implementation and effectiveness of the remedy.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fees

No stipulation.

9.1.4 Fees for Other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Business Confidential Information

Not applicable. The DoD PKI shall not collect business confidential information.

9.3.2 Information Not Within the Scope of Business Confidential Information

Not applicable. Privacy information is addressed in Section 9.4.

9.3.3 Responsibility to Protect Business Confidential Information

Not applicable.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

All Subscriber identifying information is protected by, and shall be maintained in accordance with, the Privacy Act of 1974, as implemented by DoD Directive 5400.11, *DoD Privacy Program* [DoDD 5400.11] and DoD Regulation 5400.11-R, *DoD Privacy Program* [DoD 5400.11-R].

9.4.2 Information Treated as Private

When a CMA requests non-certificate information (e.g., identifying numbers, business or home addresses and telephone numbers) from the Subscriber, the CMA shall ensure that a Privacy Act Statement is furnished the Subscriber as provided for in [DoD 5400.11-R]. Such information will only be used to manage the certificates within an organization. Such information may only be disclosed, either within or without the Department, as authorized by [DoD 5400.11-R].

9.4.3 Information Not Deemed Private

A certificate may contain information that is relevant and to effect secure transactions with the certificate. Such information may include, but is not limited to, Subscriber's Name, Subscriber Organization, Subscriber e-mail address, Subscriber EDI PI, etc. Such information may only be disclosed, either within or without the Department, as authorized by [DoD 5400.11-R].

9.4.4 Responsibility to Protect Private Information

No stipulation.

9.4.5 Notice and Consent to Use Private Information

DoD is not required to provide any notice or obtain the consent of the Subscriber in order to release the Subscriber information provided release, either within or without the Department, is authorized by [DoD 5400.11-R].

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

A CMA shall not disclose Subscriber sensitive information to any third party except as authorized by [DoD 5400.11-R]. Disclosure in response to an order of a court of competent jurisdiction or where disclosure is required by the Freedom of Information Act constitute examples of authorized releases.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 INTELLECTUAL PROPERTY RIGHTS

The US DoD shall retain ownership and all intellectual property rights for any public key certificates and private keys that it issues.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA Representations and Warranties

A CA who issues certificates that assert a policy defined in this document shall conform to the stipulations of this document, including:

- providing to the PMA a CPS, as well as any subsequent changes, for conformance assessment;
- conforming to the stipulations of the approved CPS;
- ensuring that registration information is accepted only from RAs who understand and are obligated to comply with this policy;
- including only valid and appropriate information in the certificate, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate;
- ensuring that obligations are imposed on Subscribers in accordance with Section 9.6.3, and informing Subscribers of the consequences of not complying with those obligations;
- revoking the certificates of Subscribers found to have acted in a manner counter to those obligations;
- ensuring that obligations are imposed on non-US Government Subscribers in accordance with the provisions of Section 9.8; and,
- operating or providing for the services of an on-line repository that satisfies the obligations under Section 2, and informing the repository service provider of those obligations if applicable.

A CA who is found to have acted in a manner inconsistent with these obligations is subject to action as described in Section 8.5.

9.6.2 RA Representations and Warranties

An RA who performs registration functions as described in this policy shall comply with the stipulations of this policy, and comply with a CPS approved by the DoD PMA for use with this policy. An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities.

The division of PKI duties between the CA and RA may vary among implementations of this certificate policy as provided in the CA's CPS. For example, the RA may collect information for the CA only, or it may build the certificate for the CA to sign. CAs are ultimately responsible for ensuring that the certificates they sign are generated and managed in accordance with this Policy, and shall ensure that certificate generation, management, and revocation functions are performed only by those who understand the associated certificate policy requirements, and who agree to abide by them. Security requirements imposed on the CA are likewise imposed on any RAs to the extent that the RAs are responsible for the information collected.

9.6.3 Subscriber Representations and Warranties

Subscribers shall:

- accurately represent themselves in all communications with the PKI;
- protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements, and local procedures;
- notify, in a timely manner, the CMA that issued their certificates of suspicion that their private keys are compromised or lost. Such notification shall be made directly, or indirectly through mechanisms consistent with the CA's CPS;
- abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates; and,
- use certificates provided by the DoD PKI only for transactions related to DoD business.

PKI Sponsors (as described in Section 5.2.1.4) assume the obligations of Subscribers for the certificates associated with their components.

9.6.4 Relying Party Representations and Warranties

Parties who rely upon the certificates issued under a policy defined in this document shall:

- use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension);
- check each certificate for validity, using procedures described in the X.509 standard [ISO 9594-8], prior to reliance;
- establish trust in the CA who issued a certificate by verifying the certificate path in accordance with the guidelines set by the X.509 Version 3 Amendment; and,
- preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data. Note: data format changes associated with application upgrades will often invalidate digital signatures and shall be avoided.

9.6.5 Representations and Warranties of Other Participants

Repositories that support a CA in posting information as required by this policy shall:

- maintain availability of the information as required by the certificate information posting and retrieval stipulations of this policy; and,
- provide access control mechanisms sufficient to protect repository information as described in Section 2.4.

An OCSP Responder that has been issued a DoD PKI certificate shall conform to the stipulations of this document including operating under a CPS that has been approved by the PMA. Such OCSP Responders

who are found to have acted in a manner inconsistent with these obligations are subject to action as described in Section 8.5.

All OCSP Responders that provide DoD relying parties with revocation status for certificates that assert a policy defined in this document shall conform to the following:

- Providing to the PMA a CPS, as well as any subsequent changes;
- Conforming to the stipulations of the submitted CPS;
- Ensuring that certificate and revocation information is accepted only from valid DoD approved CAs; and,
- Maintaining evidence that due diligence was exercised in validating the certificate status.

9.7 DISCLAIMERS OF WARRANTIES

No stipulation.

9.8 LIMITATIONS OF LIABILITY

A non-US Government Subscriber or entity will have no claim against the DoD arising from or relating to any certificate issued by a DoD CA or a CMA's determination to terminate a certificate. DoD is not liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages.

9.9 INDEMNITIES

No stipulation.

9.10 TERM AND TERMINATION

9.10.1 Term

This CP shall remain in effect until either a new DoD X.509 CP is approved by the PMA or the DoD PKI is terminated.

9.10.2 Termination

This CP shall survive any termination of the CA. The requirements of this CP remain in effect through the end of the archive period for the last certificate issued.

9.10.3 Effect of Termination and Survival

The responsibilities for protecting business confidential and personal information, and DoD's intellectual property rights shall survive termination of this CP.

Intellectual property rights shall survive this CP in accordance with the IP laws of the United States.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Any CMA may be removed from their duties by their supervisor. Notice is effective when given; oral notification will be confirmed in writing.

If the termination is for convenience, contract expiration, re-organization, or other non-security related reason, and provisions have been made to continue compromise recovery within the timeframes specified in Section 5.7.4 (including destruction or continued protection of signing key), compliance and security audit, archive, and data recovery services, then neither the terminated CAs certificate, nor certificates signed by that CA, need to be revoked.

If provisions for maintaining these services cannot be made, then the CA termination will be handled as a CA compromise in accordance with Sections 5.7.3 and 5.7.4.

Prior to CA termination, CAs shall provide archived data to a PMA approved DoD archival facility.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

The PMA shall review this policy at least once every year. Errors, updates, or suggested changes to this document shall be communicated to the contact in Section 1.5.2. Such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

The PMA for this policy shall publish information (including this policy) on a web site, consistent with DoD policies regarding web site contents.

The PMA will maintain a list of CAs asserting this policy (this responsibility may be delegated to a Root- or Intermediate-CA in practice). Certificate Policy updates shall be sent to those CAs. The CMA shall notify its Subscribers of any changes to the certificate policy via a mechanism described in its CPS.

9.12.2 Notification Mechanism and Period

All policy changes under consideration by the PMA shall be disseminated to interested parties for a period of at least one month.

The PMA shall accept, accept with modifications, or reject the proposed change after completion of the review period.

9.12.3 Circumstances Under Which OID Must be Changed

The policy OID shall only change if the change in the CP results in a material change to the trust by the non-DoD relying parties.

9.13 DISPUTE RESOLUTION PROVISIONS

The PMA shall decide any disputes over the interpretation or applicability of the DoD PKI CP.

9.14 GOVERNING LAW

The laws of the United States of America shall govern this Policy.

9.15 COMPLIANCE WITH APPLICABLE LAW

The PKI participants shall comply with applicable laws.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

Should it be determined that one section of this policy is incorrect or invalid, the other sections shall remain in effect until the policy is updated. Requirements for updating this policy are described in Section 9.12.1. Responsibilities, requirements, and privileges of this document are merged to the newer edition upon release of that newer edition.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 OTHER PROVISIONS

No stipulation.

10 ACRONYMS AND DEFINITIONS

CA	Certification Authority
CC	Common Criteria
CMA	Certificate Management Authority
CMCS	COMSEC Material Control System
CNSS	Committee on National Security Systems
COMSEC	Communications Security
CONOP	Concept of Operations (document)
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DAA	Designated Approving Authority
DN	Distinguished Name
DoD	Department of Defense
DSA	Digital Signature Algorithm
DSS	Digital Signature Standard
EAL	Evaluation Assurance Level
FIPS	Federal Information Processing Standard
FPKI	Federal Public Key Infrastructure
GS	General Schedule (Federal civilian level)
HAG	High Assurance Guard
I&A	Identification and Authentication
ICRL	Indirect Certificate Revocation List
ID	Identity (also, a credential asserting an identity)
INE	In-Line Network Encryptor
IP	Internet Protocol
ISSO	Information System Security Officer
KEA	Key Exchange Algorithm
KMI	Key Management Infrastructure
KRP	Key Recovery Policy
MD	Maryland
NIPRNET	Non-classified Internet Protocol Router Network
NSA	National Security Agency
NSSI	National Security System Information
NSTISSI	National Security Telecommunications and Information Systems Security Instruction
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PAA	Policy Approving Authority
PCA	Policy Creation Authority
PIN	Personal Identification Number
PKCS	Public Key Certificate Standard
PKI	Public Key Infrastructure
PMA	Policy Management Authority
RA	Registration Authority
RD	Road
RSA	Rivest, Shamir, Adleman (encryption algorithm)
S/MIME	Secure Multipurpose Internet Mail Extensions
SBU	Sensitive But Unclassified
SCI	Sensitive Compartmented Information
SIPRNET	Secret Internet Protocol Router Network
STE	Suite
TA	Trusted Agent
TSDM	Trusted System Development Methodology
US	United States

The primary source of definitions is the *National Information Assurance (IA) Glossary* [CNSS 4009]; other sources were used if [CNSS 4009] had no entry for the term, or if another source gave a definition more appropriate to PKI. If no reference is given, the definition is ad hoc.

access	Ability to make use of any information system (IS) resource. [CNSS 4009]
access control	Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [CNSS 4009]
accreditation	Formal declaration by a Designated Approving Authority that an IS is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [CNSS 4009]
applicant	The Subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG, footnote 32]
Approving Authority	Senior-level official within a U.S. Service, DoD Agency, or Civil Department/Agency who is responsible for approving the establishment of CA operations within their respective organizations.
archive	Long-term, physically separate storage.
Attribute Authority	An entity recognized by a CMA as having the authority to verify the association of attributes to an identity.
audit	Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [CNSS 4009]
audit data	Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [CNSS 4009, "audit trail"]
authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [CNSS 4009]
Auto Issuance CA	A subordinate CA that only issues certificates to non-human system components using an automated issuance process.
backup	Copy of files and programs made to facilitate recovery if necessary. [CNSS 4009]
binding	Process of associating two related elements of information. [CNSS 4009]
biometric	A physical or behavioral characteristic of a person.
Certificate Management Authority (CMA)	A Certification Authority, Registration Authority, Local Registration Authority, or OCSP Responder that has been issued a DoD PKI certificate.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Certification Authority (CA)	An authority trusted by one or more users to create and assign certificates. [ISO 9594-8]

CA facility	The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation.
certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]
certificate-related information	Information, such as a Subscriber's postal address, that is not included in a certificate, but that may be used by a CA in certificate management.
client (application)	A system entity, usually a computer process acting on behalf of a human user, that makes use of a service provided by a server.
compromise	Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [CNSS 4009]
confidentiality	Assurance that information is not disclosed to unauthorized entities or processes. [CNSS 4009]
CRL Scope	The set of certificates that could appear on a given CRL. Each CRL has a particular scope. For example, the scope could be "all certificates issued by CA X", "all CA certificates issued by CA X", "all certificates issued by CA X that have been revoked for reasons of key compromise and CA compromise", or a set of certificates based on arbitrary local information, such as "all certificates issued to the NIST employees located in Boulder". [RFC 5280]
cryptographic module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS 140]
cryptoperiod	Time span during which each key setting remains in effect. [CNSS 4009]
dual use certificate	A certificate that is intended for use with both digital signature and data encryption services.
e-commerce	The use of network technology (especially the Internet) to buy or sell goods and services.
encrypted network	A network that is protected from outside access by NSA approved high-grade (Type I) cryptography.
encryption certificate	A certificate containing a public key that is used to encrypt or decrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes. The process of storing protecting and escrowing the private component of the key pair associated with the encryption certificate is sometimes referred to as key management.
firewall	Gateway that limits access between networks in accordance with local security policy. [CNSS 4009]

High Assurance Guard (HAG)	An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance.
High Volume Responder	See OCSP Responder.
Information System Security Officer (ISSO)	Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [CNSS 4009]
insider threat	An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service.
integrity	Protection against unauthorized modification or destruction of information. [CNSS 4009]
intellectual property	Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation.
intermediate CA	A CA that is subordinate to another CA, and has a CA subordinate to itself.
key escrow	The retention of the private component of the key pair associated with a Subscriber's encryption certificate to support key recovery.
key exchange	The process of exchanging public keys (and other information) in order to establish secure communication.
key generation material	Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys.
Local Registration Authority (LRA)	A type of Registration Authority with responsibility for a local community.
Mission Assurance Category	Applicable to DoD information systems, the mission assurance category reflects the importance of information relative to the achievement of DoD goals and objectives, particularly the warfighters' combat mission. Mission assurance categories are primarily used to determine the requirements for availability and integrity. The Department of Defense has three defined mission assurance categories: Mission Assurance Category I (MAC I). Systems handling information that is determined to be vital to the operational readiness or mission effectiveness of deployed and contingency forces in terms of both content and timeliness. The consequences of loss of integrity or availability of a MAC I system are unacceptable and could include the immediate and sustained loss of mission effectiveness. Mission Assurance Category I systems require the most stringent protection measures. Mission Assurance Category II (MAC II). Systems handling information that is important to the support of deployed and contingency forces. The consequences of loss of integrity are unacceptable. Loss of availability is difficult to deal with and can only be tolerated for a short time. The consequences could include delay or degradation in providing important support services or commodities that may seriously impact mission effectiveness or operational readiness. Mission Assurance

	Category II systems require additional safeguards beyond best practices to ensure adequate assurance. Mission Assurance Category III (MAC III). Systems handling information that is necessary for the conduct of day-to-day business, but does not materially affect support to deployed or contingency forces in the short-term. The consequences of loss of integrity or availability can be tolerated or overcome without significant impacts on mission effectiveness or operational readiness. The consequences could include the delay or degradation of services or commodities enabling routine activities. Mission Assurance Category III systems require protective measures, techniques or procedures generally commensurate with commercial best practices.
naming authority	An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain.
National Security System	Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [CNSS 4009]
NIPRNET	Non-classified Internet Protocol Router Network; part of the Defense Information Infrastructure.
non-repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [CNSS 4009]
OCSP Responder	A trusted entity that provides on-line revocation status of certificates to Relying Parties. The OCSP Responder is either explicitly trusted by the Relying Party, or through a CA that Relying Party trusts, or through the CA that issued the certificate whose revocation status is being sought. An OCSP Responder is identified as a High Volume Responder if it is expected to support 100,000 or more Relying Parties. All other Responders are identified as Low Volume.
outside threat	An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service.
physically isolated network	A network that has no electronic connection to individuals outside a physically controlled space.
PKI Sponsor	Fills the role of a Subscriber for non-human system components or organizations that are named as public key certificate subjects, and is responsible for meeting the obligations of Subscribers as defined throughout this document.
Policy Management Authority (PMA)	Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies.

privacy	State in which data and system access is restricted to the intended user community and target recipient(s).
Public Key Infrastructure (PKI)	Framework established to issue, maintain, and revoke public key certificates.
Registration Authority (RA)	Entity responsible for identification and authentication of certificate subjects that have automated equipment for the communication of applicant data to Certification Authorities and does not sign or directly revoke certificates.
Root CA	In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
re-key (a certificate)	To create a new certificate with the same name and authorizations as the old one, but with a new key, extended validity period and new serial number.
Relying Party	A person who has received a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them. [ABADSG]
renew (a certificate)	To create a new certificate with the same name, key and authorizations as the old one, but with an extended validity period and new serial number.
repository	A trustworthy system for storing and retrieving certificates or other information relevant to certificates. [ABADSG] A repository may be a single system or multiple distributed systems acting as a single logical system.
risk	An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result.
risk tolerance	The level of risk an entity is willing to assume in order to achieve a potential desired result.
server	A system entity that provides a service in response to requests from clients.
signature certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
SIPRNET	Secret Internet Protocol Router Network; part of the Defense Information Infrastructure.
subordinate CA	In a hierarchical PKI, a CA whose certificate signing key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA.)
Subscriber	An entity that (1) is the subject named or identified in a certificate issued to such an entity, and (2) holds a private key that corresponds to a public key listed in that certificate. [ABADSG] Current Subscribers possess valid DoD-issued certificates.
superior CA	In a hierarchical PKI, a CA who has certified the certificate signing key of another CA, and who constrains the activities of that CA. (See subordinate CA.)

system equipment configuration	A comprehensive accounting of all system hardware and software types and settings.
system high	The highest security level supported by an information system. [CNSS 4009]
technical non-repudiation	The contribution public key mechanisms make to the provision of technical evidence supporting a non-repudiation security service.
threat	Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [CNSS 4009]
Trust Anchor	See Trusted Certificate.
trust list	Collection of Trusted Certificates used by relying parties to authenticate other certificates.
Trusted Agent	Entity authorized to act as a representative of a Certificate Management Authority in performing Subscriber identity validation during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure, authenticated delivery. The public keys included in Trusted Certificates are used to start certification paths. Also known as a "trust anchor."
Trusted Timestamp	A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time.
two person control	Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements. [CNSS 4009]
update (a certificate)	The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate.
zeroize	A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS 140]

11 REFERENCES

The following documents are referenced in this policy:

ABADSG	American Bar Association, *Digital Signature Guidelines,* 1 August 1996.
CNSS 4005	NSTISSI 4005, *Safeguarding Communications Security (COMSEC) Facilities and Material*, August 1997 (with amendments).
CNSS 4009	CNSS Instruction 4009, *National Information Systems Security Glossary,* May 2003.
DoD 5400.11-R	DoD Regulation 5400.11, *DoD Privacy Program*, 14 May 2007.
DoDD 5015.2	DoD Directive 5015.2, *DoD Records Management Program*, 21 November 2003.
DoDD 5400.11	DoD Directive 5400.11, *DoD Privacy Program*, 8 May 2007.
DoDD 8500.1	DoD Directive 8500.1, *Information Assurance (IA),* 24 October 2002.
DoDI 8500.2	DoD Instruction 8500.2, *Information Assurance (IA) Implementation,* 6 February 2003.
FIPS 140	FIPS PUB 140, *Security Requirements for Cryptographic Modules*, 25 May 2001 (current version).
FIPS 186-2	FIPS PUB 186-2, *Digital Signature Standard*, 27 January 2000.
FPKI-Prof	*Federal PKI X.509 Certificate and CRL Extensions Profile*, Version 6, 12 October 2005.
INT-SPEC	*DoD PKI Functional Interface Specification and Recomendations*, June 2007.
ISO 9594-8	*Information Technology-Open Systems Interconnection-The Directory: Authentication Framework*, 2005.
KRP	*Key Recovery Policy for the United States Department of Defense,* Version 3.0, 31 August 2003.
NAG 69C	*Information System Security Policy and Procedures for FORTEZZA Card Certification Authority Workstations*, February 2000.
PKCS 1	*RSA Cryptography Standard*, RSA Laboratories, 14 June 2002.
RFC 2560	*X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*, June 1999.
RFC 3647	*X.509 Internet Public Key Infrastructure Certificate Policy and Certification Practices Framework*, November 2003.
RFC 4210	*Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP),* September 2005.
RFC 5280	*Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, May 2008.
SDN 702	*Abstract Syntax for Utilization with Common Security Protocol (CSP), Version 3 X.509 Certificates, and Version 2 CRLs, Revision C,* 12 May 1999.
SDN 706	*X.509 Certificate and Certification Revocation List Profiles and Certification Path Processing Rules for MISSI Revision D,* 12 May 1999.

12 SUMMARY OF CHANGES TO DOD X.509 CERTIFICATE POLICY, VERSION 10

Change	Sections	Change Summary
2009-01	4.9.13 – 4.9.16	Added requirements for certificate suspension and restoration.